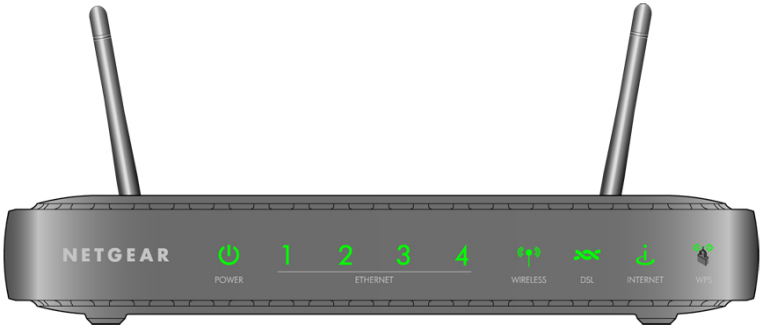
# Wireless-N ADSL2+ Modem Router DGN2000 User Manual




NETGEAR®

**NETGEAR**, Inc.
350 East Plumeria Drive
San Jose, CA 95134 USA

202-10390-02
August 2009

© 2009 by NETGEAR, Inc. All rights reserved.

## Trademarks

NETGEAR, the NETGEAR logo, and RangeMax are trademarks or registered trademarks of NETGEAR, Inc. in the United States and/or other countries. Microsoft, Windows, and Windows NT are registered trademarks and Vista is a trademark of Microsoft Corporation. Other brand and product names are trademarks or registered trademarks of their respective holders.

## Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

## Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

## Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

## European Union Statement of Compliance

Hereby, NETGEAR, Inc. declares that this modem router is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

| | |
|---|---|
| Èesky [Czech] | NETGEAR, Inc. tímto prohlašuje, že tento DGN2000 Wireless-N ADSL2+ Modem Router je ve shodì se základními požadavky a dalšími pøíslušnými ustanoveními smìrnice 1999/5/ES. |
| Dansk [Danish] | Undertegnede NETGEAR, Inc. erklærer herved, at følgende udstyr DGN2000 Wireless-N ADSL2+ Modem Router overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF. |
| Deutsch [German] | Hiermit erklärt NETGEAR, Inc., dass sich das Gerät DGN2000 Wireless-N ADSL2+ Modem Router in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet. |
| Eesti [Estonian] | Käesolevaga kinnitab NETGEAR, Inc. seadme DGN2000 Wireless-N ADSL2+ Modem Router vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele. |
| English | Hereby, NETGEAR, Inc., declares that this DGN2000 Wireless-N ADSL2+ Modem Router is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. |
| Español [Spanish] | Por medio de la presente NETGEAR, Inc. declara que el DGN2000 Wireless-N ADSL2+ Modem Router cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE. |
| Ελληνική [Greek] | ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ NETGEAR, Inc. ΔΗΛΩΝΕΙ ΟΤΙ DGN2000 Wireless-N ADSL2+ Modem Router ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ. |
| Français [French] | Par la présente NETGEAR, Inc. déclare que l'appareil DGN2000 Wireless-N ADSL2+ Modem Router est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE. |
| Italiano [Italian] | Con la presente NETGEAR, Inc. dichiara che questo DGN2000 Wireless-N ADSL2+ Modem Router è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE. |
| Latviski [Latvian] | Ar šo NETGEAR, Inc. deklarç, ka DGN2000 Wireless-N ADSL2+ Modem Router atbilst Direktîvas 1999/5/EK bûtiskajâm prasîbâm un citiem ar to saistîtajiem noteikumiem. |
| Lietuviø [Lithuanian] | Šiuo NETGEAR, Inc. deklaruoja, kad šis DGN2000 Wireless-N ADSL2+ Modem Router atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas. |

| | |
|---|---|
| Nederlands [Dutch] | Hierbij verklaart NETGEAR, Inc. dat het toestel DGN2000 Wireless-N ADSL2+ Modem Router in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG. |
| Malti [Maltese] | Hawnhekk, NETGEAR, Inc., jiddikjara li dan DGN2000 Wireless-N ADSL2+ Modem Router jikkonforma mal-tiijiet essenzjali u ma provvedimenti orajn relevanti li hemm fid-Dirrettiva 1999/5/EC. |
| Magyar [Hungarian] | Alulírott, NETGEAR, Inc. nyilatkozom, hogy a DGN2000 Wireless-N ADSL2+ Modem Router megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak. |
| Polski [Polish] | Niniejszym NETGEAR, Inc. oœwiadcza, ¿e DGN2000 Wireless-N ADSL2+ Modem Router jest zgodny z zasadniczymi wymogami oraz pozosta³ymi stosownymi postanowieniami Dyrektywy 1999/5/EC. |
| Português [Portuguese] | NETGEAR, Inc. declara que este DGN2000 Wireless-N ADSL2+ Modem Router está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE. |
| Slovensko [Slovenian] | NETGEAR, Inc. izjavlja, da je ta DGN2000 Wireless-N ADSL2+ Modem Router v skladu z bistvenimi zahtevami in ostalimi relevantnimi doloèili direktive 1999/5/ES. |
| Slovensky [Slovak] | NETGEAR, Inc. týmto vyhlasuje, že DGN2000 Wireless-N ADSL2+ Modem Router spåòa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES. |
| Suomi [Finnish] | NETGEAR, Inc. vakuuttaa täten että DGN2000 Wireless-N ADSL2+ Modem Router tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. |
| Svenska [Swedish] | Härmed intygar NETGEAR, Inc. att denna *[utrustningstyp]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG. |

A printed copy of the EU Declaration of Conformity certificate for this product is provided in the DGN2000 product package.

## Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das DGN2000 Wireless-N ADSL2+ Modem Router gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

## Certificate of the Manufacturer/Importer

It is hereby certified that the DGN2000 Wireless-N ADSL2+ Modem Router has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

## Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

## Customer Support

Refer to the Support Information Card that shipped with your DGN2000 Wireless-N ADSL2+ Modem Router.

## World Wide Web

NETGEAR maintains a World Wide Web home page that you can access at the universal resource locator (URL) *http://www.netgear.com*. A direct connection to the Internet and a Web browser such as Internet Explorer are required.

## Product and Publication Details

| | |
|---|---|
| **Model Number:** | DGN2000 |
| **Publication Date:** | August 2009 |
| **Product Family:** | Modem Router |
| **Product Name:** | DGN2000 Wireless-N ADSL2+ Modem Router |
| **Home or Business Product:** | Home |
| **Language:** | English |
| **Publication Part Number:** | 202-10390-02 |
| **Publication Version Number:** | 1.0 |

# Contents


## Wireless-N ADSL2+ Modem Router DGN2000 User Manual

**About This Manual**

Conventions, Formats, and Scope ..... xi
Revision History ..... xii

**Chapter 1**
**Connecting Your Modem Router to the Internet**

Using the Setup Manual ..... 1-1
What You Need before You Begin ..... 1-2
Logging In to the Modem Router ..... 1-2
Auto-Detecting Your Internet Connection ..... 1-4
Viewing or Manually Configuring Your ISP Settings ..... 1-6
Understanding the Basic Settings Screen ..... 1-7
ADSL Settings ..... 1-9
How the Internet Connection Works ..... 1-10

**Chapter 2**
**Configuring Your Wireless Network and Security Settings**

Planning Your Wireless Network ..... 2-1
Wireless Placement and Range Guidelines ..... 2-2
Wireless Security Options ..... 2-3
Manually Configuring Your Wireless Network ..... 2-4
Manually Configuring Your Wireless Security ..... 2-9
Restricting Wireless Access to Your Network ..... 2-9
Configuring Mixed WPA-PSK+WPA2-PSK Security ..... 2-12
Choosing Alternative Authentication and Encryption Methods ..... 2-13
Using Push 'N' Connect (WPS) to Configure Your Wireless Network and Security ..... 2-16
Connecting Additional Wireless Client Devices After WPS Setup ..... 2-19

**Chapter 3**
**Protecting Your Network**

Protecting Access to Your Modem Router ....3-1
Changing the Built-In Password ....3-2
Changing the Administrator Login Time-out ....3-3
Blocking Keywords, Sites, and Services ....3-3
Firewall Rules ....3-5
Inbound Rules (Port Forwarding) ....3-6
Outbound Rules (Service Blocking) ....3-9
Order of Precedence for Rules ....3-11
Services ....3-12
Setting Times and Scheduling Firewall Services ....3-13
Setting Your Time Zone ....3-13
Scheduling Firewall Services ....3-15

**Chapter 4**
**Managing Your Network**

Backing Up, Restoring, and Erasing Your Settings ....4-1
Backing Up the Configuration to a File ....4-1
Restoring the Configuration from a File ....4-2
Erasing the Configuration ....4-2
Upgrading the Modem Router Firmware ....4-3
Network Management Information ....4-4
Viewing the Modem Router Status and Usage Statistics ....4-4
Viewing Attached Devices ....4-9
Viewing, Selecting, and Saving Logged Information ....4-10
Examples of Log Messages ....4-12
Enabling Security Event E-mail Notification ....4-13
Running Diagnostic Utilities and Rebooting the Modem Router ....4-14
Configuring Remote Management ....4-15
Automatic Firmware Recovery ....4-17

**Chapter 5**
**Advanced Configuration**

Configuring WAN Settings ....5-1
Setting Up a Default DMZ Server ....5-1
Other WAN Options ....5-2

Setting up Quality of Service (QoS) ....5-3
Configuring QoS for Internet Access ....5-4
Editing or Deleting an Existing QoS Policy ....5-7
Configuring LAN IP Settings ....5-7
Configuring DHCP ....5-9
Configuring Dynamic DNS ....5-11
Using Static Routes ....5-12
Static Route Example ....5-12
Configuring Static Routes ....5-13
Configuring Universal Plug and Play ....5-15
Building Wireless Bridging and Repeating Networks ....5-16
Point-to-Point Bridge Configuration ....5-18
Multi-Point Bridge ....5-19
Repeater with Wireless Client Association ....5-21
Displaying and Configuring Advanced WPS Settings ....5-22

**Chapter 6**
**Troubleshooting**

Basic Functioning ....6-1
“Welcome” Page Displays instead of Router Main Menu ....6-2
Power LED Is Off ....6-2
Power LED Is Red ....6-2
LAN or ADSL Port LED Is Off ....6-3
Window Appears Asking You to Reload Firmware ....6-3
Cannot Log in to the Modem Router ....6-3
Troubleshooting the ISP Connection ....6-4
ADSL Link ....6-4
Internet LED is Red ....6-5
Obtaining an Internet IP Address ....6-6
Troubleshooting PPPoE or PPPoA ....6-6
Troubleshooting Internet Browsing ....6-7
Resolving a ‘Reload Firmware’ Message ....6-7
Troubleshooting a TCP/IP Network Using the Ping Utility ....6-8
Testing the LAN Path to Your Modem Router ....6-8
Testing the Path from Your Computer to a Remote Device ....6-9
Restoring the Default Configuration and Password ....6-10

Using the Wireless On/Off and WPS Buttons to Reset the Router .....6-10
Problems with Date and Time .....6-10

**Appendix A**
**Technical Specifications**

General Specifications ..... A-1
Default Configuration ..... A-2

**Appendix B**
**Related Documents**

**Index**

# About This Manual

The *NETGEAR® Wireless-N ADSL2+ Modem Router DGN2000 User Manual* describes how to install, configure and troubleshoot the DGN2000 Wireless-N ADSL2+ Modem Router. The information in this manual is intended for readers with intermediate computer and Internet skills.

## Conventions, Formats, and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical Conventions**. This manual uses the following typographical conventions::

| | |
|---|---|
| *Italic* | Emphasis, books, CDs, file and server names, extensions |
| **Bold** | User input, IP addresses, GUI screen text |
| `Fixed` | Command prompt, CLI text, code |
| *italic* | URL links |

- **Formats**. This manual uses the following formats to highlight special messages:

| | |
|---|---|
| | **Note:** This format is used to highlight information of importance or special interest. |

| | |
|---|---|
| | **Tip:** This format is used to highlight a procedure that will save time or resources. |

| | |
|---|---|
| | **Warning:** Ignoring this type of note may result in a malfunction or damage to the equipment. |

- **Scope**. This manual is written for the Wireless-N ADSL2+ Modem Router according to these specifications:

| | |
|---|---|
| Product Version | DGN2000 Wireless-N ADSL2+ Modem Router |
| Manual Publication Date | August 2009 |

For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in Appendix B, "Related Documents."

**Note:** Product updates are available on the NETGEAR, Inc. website at *http://kbserver.netgear.com/products/DGN2000.asp*.

## Revision History

| Part Number | Version Number | Date | Description |
|---|---|---|---|
| 208-10255-02 | 1.0 | August 2009 | QoS and WPS disable features added. |
| 208-10255-01 | 1.0 | July 2008 | Original publication. |

# Chapter 1
# Connecting Your Modem Router to the Internet

This chapter describes how to configure your DGN2000 Wireless-N ADSL2+ Modem Router Internet connection. When you perform the initial configuration of your modem router using the *Resource CD* as described in the *Wireless-N ADSL2+ Modem Router DGN2000 Setup Manual*, these settings are configured automatically for you. This chapter provides further details about these settings, as well as instructions on how to log in to the modem router for further configuration.

**Note:** NETGEAR recommends using the Smart Wizard on the *Resource CD* for initial configuration, as described in the *Wireless-N ADSL2+ Modem Router DGN2000 Setup Manual*.

This chapter includes:


- "Using the Setup Manual"
- "What You Need before You Begin" on page 1-2"
- "Logging In to the Modem Router" on page 1-2"
- "Auto-Detecting Your Internet Connection" on page 1-4"
- "Viewing or Manually Configuring Your ISP Settings" on page 1-6"
- "ADSL Settings" on page 1-9"
- "How the Internet Connection Works" on page 1-10"


## Using the Setup Manual

For first-time installation of your modem router, refer to the *Wireless-N ADSL2+ Modem Router DGN2000 Setup Manual*. The Setup Manual explains how to launch the NETGEAR Smart Wizard on the *Resource CD* to step you through the procedure to connect your router, modem, and computers. The Smart Wizard will assist you in configuring your wireless settings and enabling wireless security for your network. After initial configuration using the Setup Manual, you can use the information in this Reference Manual to configure additional features of your wireless router.

For installation instructions in a language other than English, see the language options on the *Resource CD*.

## What You Need before You Begin

You need to prepare the following before you can set up your firewall:

- Active Internet service provided by an ADSL account
- The Internet Service Provider (ISP) configuration information for your ADSL account
  - ISP login name and password
  - ISP Domain Name Server (DNS) addresses
  - Fixed or static IP address
  - Host and domain names
- Depending on how your ISP set up your Internet account, you need to know one or more of these settings:
  - Virtual path identifier (VPI) and Virtual channel identifier (VCI) parameters
  - Multiplexing method
  - Host and domain names
- ASDL microfilters as explained in the *Wireless-N ADSL2+ Modem Router DGN2000 Setup Manual*

In addition, your computer must be set up to use DHCP to get its TCP/IP configuration from the modem router. This is usually the case. For help with DHCP, see the documentation that came with your computer, or see the link to the online document that you can access from "Preparing Your Network" in Appendix B.

Your ISP should have provided you with all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide it.

## Logging In to the Modem Router

You can log in to the modem router to view or change its settings.

**Note:** Your computer must be configured for DHCP. For help with configuring DHCP, see the documentation that came with your computer or see the link to the online document that you can access from "Preparing Your Network" in Appendix B.

To log in to the modem router:

1. Type **http://routerlogin.net** or **http://192.168.0.1** in the address field of an Internet browser.

**Figure 1-1**

A login window similar to the following opens:

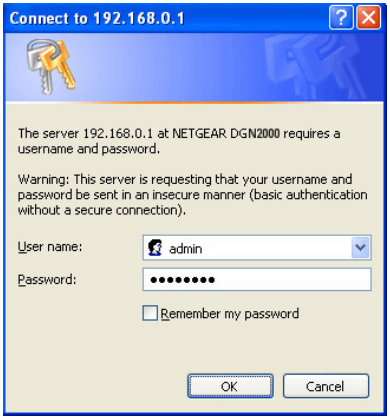

Connect to 192.168.0.1
The server 192.168.0.1 at NETGEAR DGN2000 requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

**Figure 1-2**

2. Enter **admin** for the user name and **password** for the password, both in lower case letters.
3. Select Setup Wizard to go to the Setup Wizard screen:

Setup Wizard
Setup Wizard
Select Country and Language
Country:
USA
Language:
English
Auto-Detect Connection Type
This Setup Wizard can detect the type of Internet connection you have.
Do You want The Smart Setup Wizard To try And detect The connection type now?
Yes.
No. I want to configure The Router myself.
Next

**Figure 1-3**

This screen includes the following:

- **Country**. It is important to specify the location where the modem router will operate so that the Internet connection will work correctly.
- **Language**. You can select a language from the drop-down list.
- **Auto-Detect Connection Type**. If you want to change the settings for the Internet connection, select **Yes** or **No**, and then click **Next**.
  - **Yes**. Let the modem router Setup Wizard auto-detect the type of Internet connection that you have and configure it. See the next section, "Auto-Detecting Your Internet Connection."
  - **No, I want to Configure the Router Myself**. Enter your Internet settings manually in the Basic Settings screen. See "Understanding the Basic Settings Screen" on page 1-7.

  In either case, use the configuration settings that your ISP provided to assure that the configuration for your Internet connection is correct.
- **Test**. To test your Internet connection, click **Test**. If the NETGEAR website does not appear within 1 minute, see Chapter 6, "Troubleshooting."

## Auto-Detecting Your Internet Connection

The Smart Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration.

**Note:** The wizard cannot detect a PPTP connection with your ISP. If your ISP uses this protocol, then you must configure your connection manually (see "Understanding the Basic Settings Screen" on page 1-7).

To use the Smart Setup Wizard to assist with configuration or to view the Internet connection settings:

1. From the Setup Wizard screen, select **Yes** for the Auto-Detect Connection Type, and then click **Next** to proceed.

The Setup Wizard detects your ISP configuration. Depending on the type of connection, you are prompted to enter your ISP settings, as shown in the following table.

**Table 1-1. Auto-Detected Internet Connection Types**

| Connection Type | ISP Information |
|---|---|
| PPP over Ethernet (PPPoE)<br>PPP over ATM (PPPoA) | Enter the login user name and password. These fields are case-sensitive. |
| Dynamic IP Account Setup | No entries needed. |
| IP over ATM Classical IP assignment (RFC1577) | • Enter the assigned IP address, subnet mask, and the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.<br>• DNS servers are required to perform the function of translating an Internet name such as *www.netgear.com* to a numeric IP address. For a fixed IP address configuration, you must obtain DNS server addresses from your ISP and enter them manually here. |
| Fixed IP (Static) Account Setup | 1. If required, enter the account name and domain name from your ISP.<br>2. Select **Use Static IP Address** or **Use IP Over ATM** (IPoA — RFC1483 Routed) according to the information from your ISP. If you select IPoA, the router will detect the gateway IP address, but you still need to provide the router IP address.<br>3. Enter your assigned IP address, subnet mask, and the IP address of your ISP's gateway modem router. This information should have been provided to you by your ISP.<br>4. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.<br><br>DNS servers are required to perform the function of translating an Internet name such as *www.netgear.com* to a numeric IP address. For a fixed IP address configuration, you must obtain DNS server addresses from your ISP and enter them manually here. |

2. To save your settings, click **Apply**.
3. Click **Test** to verify your Internet connection. If you have trouble connecting to the Internet, see Chapter 6, "Troubleshooting."

# Viewing or Manually Configuring Your ISP Settings

NETGEAR recommends that you specify your country and language before you configure the settings on the Basic Settings screen. See "Logging In to the Modem Router" on page 1-2. You must install the ADSL filters and connect the modem router to the ADSL line as described in the *Wireless-N ADSL2+ Modem Router DGN2000 Setup Manual* before you configure the settings in the Basic Settings screen.

To view or configure the basic settings:

1. Log in to the modem router as described in "Logging In to the Modem Router" on page 1-2.
2. Select Basic Settings to display the Basic Settings screen.

   The Basic Settings screen is explained in "Understanding the Basic Settings Screen" on page 1-7.
3. Select **Yes** or **No** depending on whether your ISP requires a login. This selection changes the fields available on the Basic Settings screen.
   - **Yes**. If your ISP requires a login, select the encapsulation method. Enter the login name. If you want to change the login time-out, enter a new value in minutes.
   - **No**. If your ISP does not require a login, enter the account name, if required, and the domain name, if required.
4. Enter the settings for the IP address and DNS server.

   The default ADSL settings usually work fine. If you have problems with your connection, check the ADSL settings. See "ADSL Settings" on page 1-9 for more details.
5. If no login is required, you can specify the MAC Address setting.
6. Click **Apply** to save your settings.
7. Click **Test** to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to Chapter 6, "Troubleshooting."

**Note:** When your Internet connection is working you will no longer need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your modem router automatically logs you in.

# Understanding the Basic Settings Screen

The fields on the Basic Settings screen depend on whether or not your Internet connection requires a login.

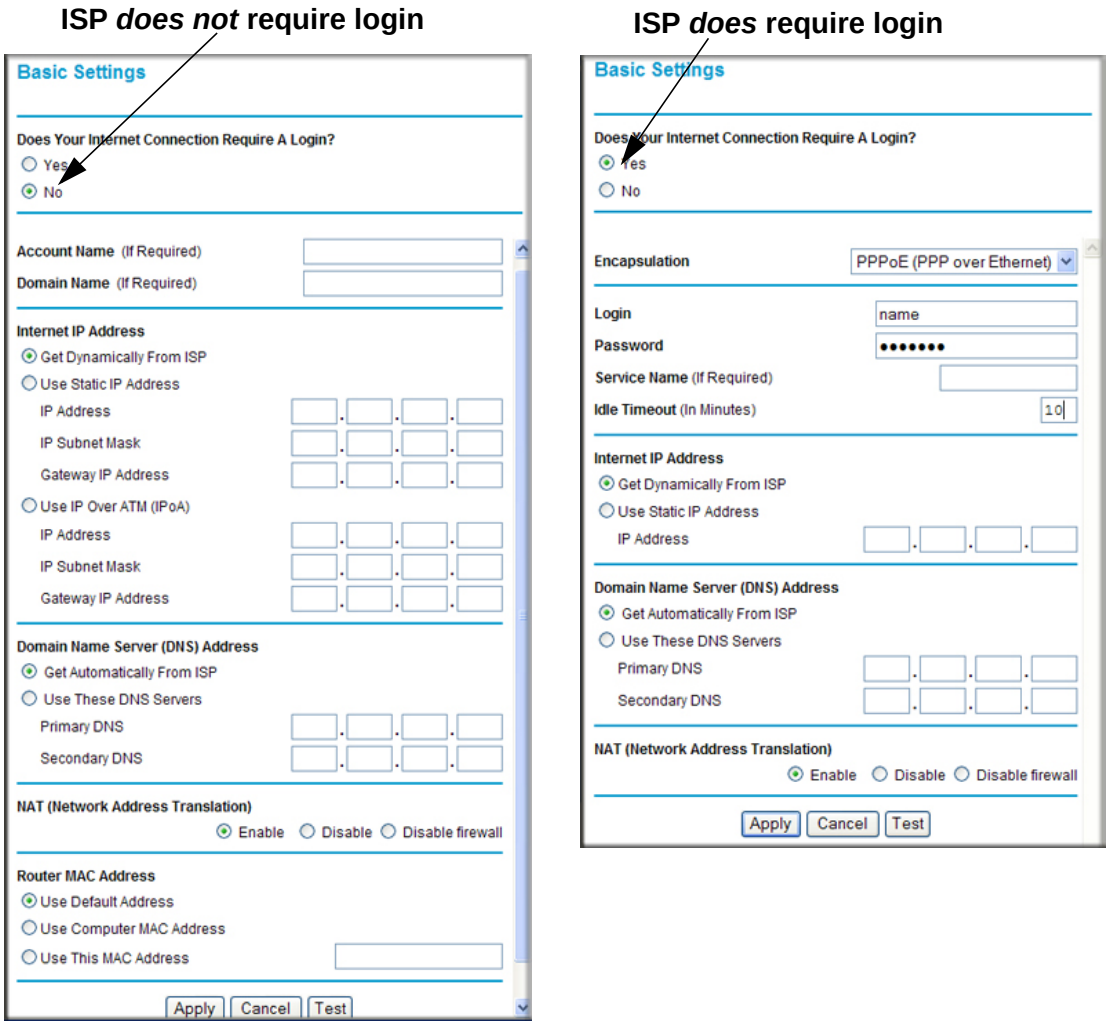



**Figure 1-4**

The following table explains the fields in the Basic Settings screen. Note that the group of fields included in this screen depends on whether or not a login is required.

**Table 1-2. Basic Settings screen fields**

| Settings | | Description |
|---|---|---|
| Does Your ISP Require a Login? | | • Yes<br>• No |
| These fields appear only if no login is required. | Account Name (If required) | Enter the account name provided by your ISP. This might also be called the host name. |
| | Domain Name (If required) | Enter the domain name provided by your ISP. |
| These fields appear only if your ISP requires a login. | Encapsulation | • PPPoE (PPP over Ethernet)<br>• PPPoA (PPP over ATM) |
| | Login | The login name provided by your ISP. This is often an e-mail address. |
| | Password | The password that you use to log in to your ISP. |
| | Idle Timeout (In minutes) | If you want to change the login time-out, enter a new value in minutes. This determines how long the modem router keeps the Internet connection active after there is no Internet activity from the LAN. Entering an Idle Timeout value of 0 (zero) means never log out. |
| Internet IP Address | | • **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.<br>• **Use Static IP Address**. Enter the IP address that your ISP assigned. Also enter the IP subnet mask and the gateway IP address. The gateway is the ISP's modem router to which your modem router will connect. |
| | This field appears only if no login is required. | • **Use IP Over ATM (IFoA)**. Your ISP uses Classical IP addresses (RFC 1577). Enter the IP address, IP subnet mask, and gateway IP addresses that your ISP assigned. |
| Domain Name Server (DNS) Address | | The DNS server is used to look up site addresses based on their names.<br>• **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.<br>• **Use These DNS Servers**. If you know that your ISP does not automatically transmit DNS addresses to the modem router during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also. |

**Table 1-2. Basic Settings screen fields (continued)**

| Settings | | Description |
|---|---|---|
| NAT (Net Address Translation) | | NAT automatically assigns private IP addresses (10.1.1.x) to LAN-connected devices.<br>• **Enable**. Usually NAT is enabled.<br>• **Disable**. This disables NAT, but leaves the firewall active. Disable NAT only if you are sure that you do not require it. When NAT is disabled, only standard routing is performed by this router. Classical routing lets you directly manage the IP addresses that the modem router uses. Classical routing should be selected only by experienced users*<br>• **Disable firewall**. This disables the firewall in addition to disabling NAT. With the firewall disabled, the protections usually provided to your network are disabled. |
| These fields appear only if no login is required. | Router MAC Address | The Ethernet MAC address that will be used by the modem router on the Internet port. Some ISPs register the Ethernet MAC address of the network interface card in your computer when your account is first opened. They will then accept traffic only from the MAC address of that computer. This feature allows your modem router to masquerade as that computer by "cloning" its MAC address.<br>• **Use Default Address**. Use the default MAC address.<br>• **Use Computer MAC Address**. The modem router will capture and use the MAC address of the computer that you are now using. You must be using the one computer that is allowed by the ISP.<br>• **Use This MAC Address**. Enter the MAC address that you want to use. |

*. Disabling NAT reboots the modem router and resets its configuration settings to the factory defaults. Disable NAT only if you plan to install the modem router in a setting where you will be manually administering the IP address space on the LAN side of the router.

# ADSL Settings

**Note:** For information about how to install ADSL filters, see the *Wireless-N ADSL2+ Modem Router DGN2000 Setup Manual*.

The default ADSL settings of your modem router work fine for most ISPs. However, some ISPs use a specific multiplexing method and virtual circuit number for the virtual path identifier (VPI) and virtual channel identifier (VCI).

**Note:** You must use the Setup Wizard to select the correct country for the default ADSL settings to work.

If your ISP provided you with a multiplexing method or VPI/VCI number, then enter the setting:

1. From the main menu, select ADSL Settings.The ADSL Settings screen displays.

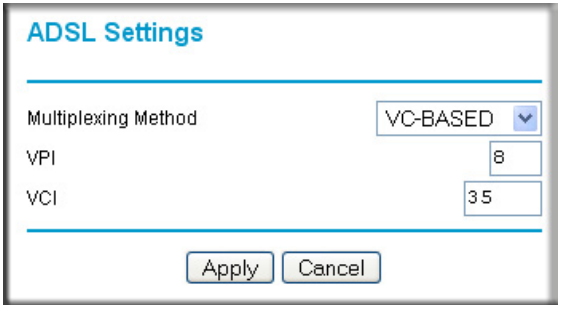



**Figure 1-5**

2. In the **Multiplexing Method** drop-down list, select **LLC-based** or **VC-based**.
3. For the VPI, type a number between 0 and 255. The default is 8.
4. For the VCI, type a number between 32 and 65535. The default is 35.
5. Click **Apply**.

## How the Internet Connection Works

Your modem router is now configured to provide Internet access for your network. Your modem router automatically connects to the Internet when one of your computers requires access. It is not necessary to run a dialer or login application such as dial-up networking or Ethernet to connect, log in, or disconnect. The modem router performs these functions automatically as needed.

To access the Internet from any computer connected to your modem router, launch an Internet browser such as Microsoft Internet Explorer. You should see the modem router's Internet LED blink, indicating communication to the ISP. The browser should begin to display a Web page.

# Chapter 2
# Configuring Your Wireless Network and Security Settings

This chapter describes how to configure the wireless features of your modem router.For a wireless connection, the SSID, also called the wireless network name, and the wireless security setting must be the same for the modem router and wireless computers or wireless adapters. NETGEAR strongly recommends that you use wireless security.

**Warning:** Computers can connect wirelessly at a range of several hundred feet. This can allow others outside of your immediate area to access your network.

This chapter includes:


- "Planning Your Wireless Network"
- "Manually Configuring Your Wireless Network" on page 2-4"
- "Manually Configuring Your Wireless Security" on page 2-9"
- "Using Push 'N' Connect (WPS) to Configure Your Wireless Network and Security" on page 2-16


## Planning Your Wireless Network

For compliance and compatibility between similar products in your area, the operating channel and region must be set correctly.

To configure the wireless network, you can either specify the wireless settings, or you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security.

- To manually configure the wireless settings, you must know the following:
  - SSID. The default SSID for the modem router is NETGEAR.
  - The wireless mode (802.11n, 802.11g, or 802.11b) that each wireless adapter supports.
  - Wireless security option. To successfully implement wireless security, check each wireless adapter to determine which wireless security option it supports.

See "Manually Configuring Your Wireless Security" on page 2-9.

- Push 'N' Connect (WPS) automatically implements wireless security on the modem router while, at the same time, allowing you to automatically implement wireless security on any WPS-enabled devices (such as wireless computers and wireless adapter cards). You activate WPS by pressing a WPS button on the modem router, clicking an on-screen WPS button, or entering a PIN number. This generates a new SSID and implements WPA/WPA2 security.

  To set up your wireless network using the WPS feature:

  – Use the WPS button on the side of the modem router (there is also an on-screen WPS button), or enter the PIN of the wireless device.
  – Make sure that all wireless computers and wireless adapters on the network are Wi-Fi certified and WPA or WPA 2 capable, and that they support WPS configuration.

  See "Using Push 'N' Connect (WPS) to Configure Your Wireless Network and Security" on page 2-16.

## Wireless Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the physical placement of the modem router. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

For best results, place your modem router according to the following guidelines:

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwave ovens, and 2.4 GHz cordless phones.
- Away from large metal surfaces.
- Put the antenna in a vertical position to provide the best side-to-side coverage. Put the antenna in a horizontal position to provide the best up-and-down coverage.
- If using multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use Channels 1 and 6, or 6 and 11).

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

## Wireless Security Options

Indoors, computers can connect over 802.11g wireless networks at a maximum range of up to 300 feet. Such distances can allow for others outside your immediate area to access your network.

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The modem router provides highly effective security features, which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

There are several ways you can enhance the security of your wireless network:

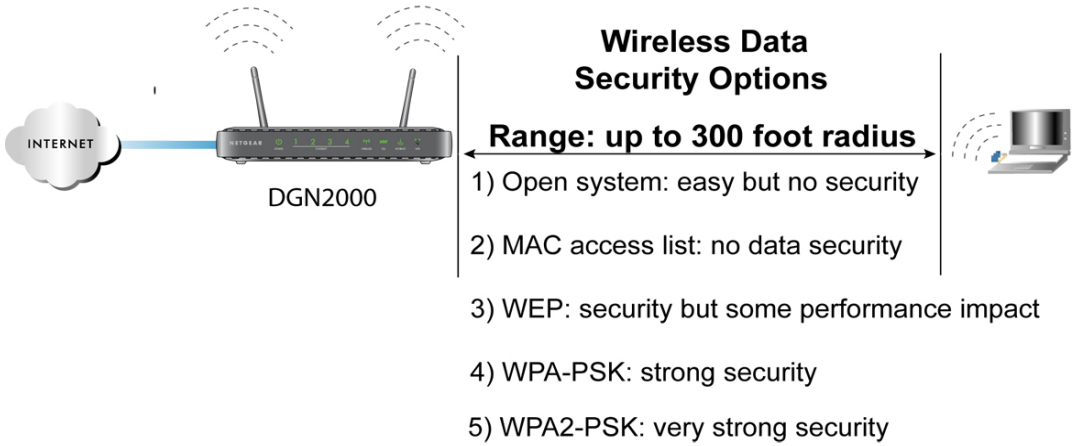

INTERNET
DGN2000
Wireless Data
Security Options
Range: up to 300 foot radius
1) Open system: easy but no security
2) MAC access list: no data security
3) WEP: security but some performance impact
4) WPA-PSK: strong security
5) WPA2-PSK: very strong security

**Figure 2-1**

There are several ways you can enhance the security of your wireless network:

- **Restrict access based on MAC address**. You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the modem router. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed (see “Restricting access by MAC address” on page 2-10).
- **Turn off the broadcast of the wireless network name SSID**. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies wireless network discovery feature of some products, such as Windows XP, but the data is still exposed (see “Hiding your wireless network name (SSID)” on page 2-10).

- **WEP**. Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK (see "Configuring WEP" on page 2-13).
- **WPA-802.1x**. Wi-Fi Protected Access (WPA) with user authentication implemented using IEE 802.1x and RADIUS servers (see "Configuring WPA-802.1x" on page 2-15).
- **WPA-PSK (TKIP) + WPA2-PSK (AES)**. Wi-Fi Protected Access (WPA) using a pre-shared key to perform authentication and generate the initial data encryption keys. The very strong authentication along with dynamic per frame re-keying of WPA makes it virtually impossible to compromise (see "Configuring Mixed WPA-PSK+WPA2-PSK Security" on page 2-12).

## Manually Configuring Your Wireless Network

You can view or manually configure the wireless settings and wireless security for the modem router in the Wireless Settings screen. If you want to make changes, make sure to note the current settings first. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

**Note:** If you use a wireless computer to change the wireless network name (SSID) or wireless security settings, you will be disconnected when you click **Apply**. To avoid this problem, use a computer with a wired connection to access the modem router.

To manually configure the wireless settings:

1. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Select Wireless Settings in the main menu. The Wireless Settings screen displays.

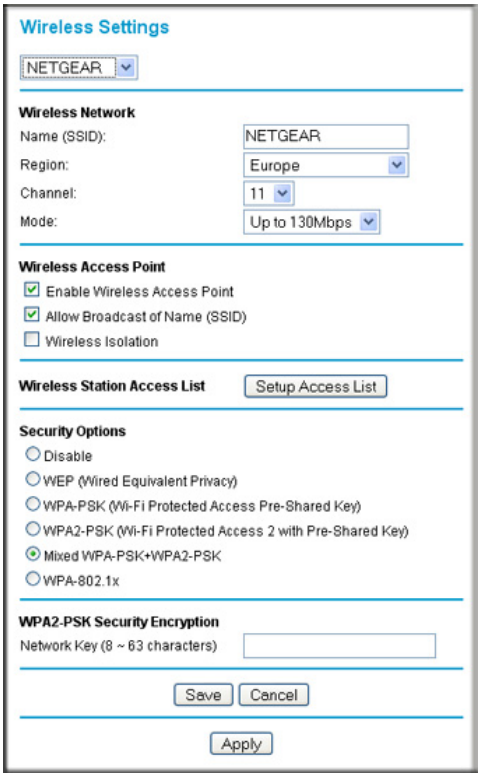



**Figure 2-2**

Table 2-1 on page 2-6 describes the information that is displayed in the Wireless Settings screen.

3. Choose a suitable descriptive name for the wireless network name (SSID). In the **SSID** field, enter a value of up to 32 alphanumeric characters. The default SSID is **NETGEAR**.

> **Note:** The SSID of any wireless access adapters must match the SSID you specify in the modem router. If they do not match, you will not get a wireless connection.

4. Select the region in which the wireless interface will operate.
5. Set the channel if necessary. The default channel is 11.

   This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby

wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your modem router. For more information about the wireless channel frequencies, see the online document that you can access from "Preparing Your Network" in Appendix B.

**Note:** Up to 270Mbps mode uses two channels, but in this mode only the first channel is listed in the channel pulldown menu. The associated channels in this mode are: 1+5, 2+6, 3+7, 4+8, 5+9, 6+10, and 7+11. When you select another wireless network mode, the channel pulldown displays all available channels: 1 through 13. However, available wireless channels depend on the selected wireless region.

6. For initial configuration and test, leave the Wireless Card Access List set to allow everyone access by making sure that **Turn Access Control On** is not selected in the Wireless Station Access List. In addition, leave the encryption strength set to **None**.
7. Click **Save** to save your settings or click **Apply** to allow your changes to take effect immediately.
8. Configure and test your computers for wireless connectivity.

   Program the wireless adapter of your computers to have the same SSID and channel that you specified in the router. Check that they have a wireless link and can obtain an IP address by DHCP from the modem router.

Once your computers have basic wireless connectivity to the modem router, you can configure the advanced wireless security functions of the firewall.

**Table 2-1. Wireless Settings**

| Settings | Description |
|---|---|
| Wireless LAN | The pulldown menu just below Wireless Settings allows for the selection of one of four wireless LANs (WLANs) with the following default names:<br>• NETGEAR<br>• NETGEAR2<br>• NETGEAR3<br>• NETGEAR4<br>You can change the default name of the selected WLAN in the Name (SSID) field.<br>Note: The region, channel, and mode can be set only for the primary wireless LAN (NETGEAR). In addition, access control can be turned on only for the primary wireless LAN. |

**Table 2-1. Wireless Settings (continued)**

| Settings | | Description |
|---|---|---|
| Wireless Network | Name (SSID) | The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. The default SSID is **NETGEAR**, but NETGEAR strongly recommends that you change your network name to a different value. Any device you that want to let participate in a wireless network must use the SSID. |
| | Region | The location where the modem router is used. Select your region. This setting will apply to any guest networks you set up. It might not be legal to operate the modem router in a region other than the regions shown here. |
| | Channel | The wireless channel: 1 through 13. This setting applies to any guest networks you set up. Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, you might need to experiment with different channels to see which is best. For Up to 130Mbps mode, the default channel is 11; for Up to 270Mbps mode, the default channel is 7. The number of available channels varies by region and depends on the selected mode. |
| | Mode<br>The mode can be set only for the primary wireless LAN (NETGEAR). | **Up to 270Mbps** This is the fastest mode, and is compatible with all 802.11g, 802.11b, and faster Draft-N wireless stations. The channel bandwidth expands from 20 MHz to 40 MHz to achieve the 270 Mbps rate. Channel expansion operates on a frame-by-frame basis to avoid interference with transmissions from other wireless networks. Two channels are used, but only the first is listed in the Channel field. The associated channels are: 1+5, 2+6, 3+7, 4+8, 5+9, 6+10, and 7+11. |
| | | **Up to 130Mbps** (default setting) Allows wireless stations that support speeds up to 130 Mbps. The router transmits two streams with different data concurrently on the same channel. This mode restricts channel bandwidth to minimize interference with the transmissions of other wireless networks. |
| | | **g & b** Older 802.11g and 802.11b wireless stations can access this device. You might want to select this mode if you have a wireless station that is using WEP security and does not support WPA-PSK or WPA2-PSK. |
| | | **g only** Only 802.11g wireless stations can access this device. |
| | | **b only** Only 802.11b wireless stations or 802.11g stations operating in 802.11b mode can access this device. |

**Table 2-1. Wireless Settings (continued)**

| Settings | | Description |
|---|---|---|
| Wireless Access Point | Enable | • Selected by default, this setting enables the wireless radio, which allows the modem router to work as a wireless access point. Turning off the wireless radio can be helpful for configuration, network tuning, or troubleshooting.<br>• The Wireless LED on the front of the modem router displays the current status of the wireless access point to let you know if it is disabled or enabled. The wireless access point must be enabled to allow wireless stations to access the Internet. |
| | Allow Broadcast of Name (SSID). | Selected by default, the modem router broadcasts its SSID, allowing wireless stations that have a null (blank) SSID to adopt the correct SSID. If you disable broadcast of the SSID, only devices with the correct SSID can connect. This nullifies the wireless network discovery feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. For this reason NETGEAR recommends that you also enable wireless security. |
| | Wireless Isolation | This feature is disabled by default. If it is enabled, wireless stations cannot communicate with each other or with stations on the wired network. |
| Wireless Station Access List | Turn Access Control On | Access control is disabled by default so that any computer configured with the correct wireless network name or SSID can access to your wireless network. For increased security, you can restrict access to the wireless network to only specific computers based on their MAC addresses. See "Restricting access by MAC address." |
| Security Options | Disable | Wireless security is not used. |
| | WEP | In WEP (Wired Equivalent Privacy) mode you can select 64-bit or 128-bit data encryption. This mode has been superseded by WPA-PSK and WPA2-PSK, which should be selected if possible. See "Configuring WEP." |
| | WPA-PSK | WPA Pre-Shared-Key (Wi-Fi Protected Access Pre-Shared Key) uses a pre-shared key to perform the authentication and generate the initial data encryption keys. Then, it dynamically varies the encryption key.<br>WPA-PSK uses TKIP (Temporal Key Integrity Protocol) data encryption, implements most of the IEEE 802.11i standard, and is designed to work with all wireless network interface cards, but not all wireless access points. See "Configuring Mixed WPA-PSK+WPA2-PSK Security." |

**Table 2-1. Wireless Settings (continued)**

| Settings | | Description |
|---|---|---|
| Security Options (continued) | WPA2-PSK | WPA Pre-Shared-Key (Wi-Fi Protected Access 2 with Pre-Shared Key) uses a pre-shared key to perform the authentication and generate the initial data encryption keys. Then, it dynamically varies the encryption key. WPA2-PSK provides the best throughput with 802.11N because the encryption is supported in the hardware. WPA2-PSK uses AES (Advanced Encryption Standard) data encryption, implements the full IEEE 802.11i standard, but does not work with some older network cards. See "Configuring Mixed WPA-PSK+WPA2-PSK Security." |
| | Mixed WPS-PSK+ WPA2-PSK | Mixed WPA-PSK + WPA2-PSK uses both WPA-PSK + WPA2-PSK standard encryption. A high performance client such as the NETGEAR WN511B should connect using WPA2-PSK in order to achieve maximum performance. Wireless clients that connect to this router using WPA-PSK will run at reduced performance levels. See "Configuring Mixed WPA-PSK+WPA2-PSK Security." |
| | WPA-802.1x | In WPA-802.1x mode, user authentication is implemented using 802.1x and RADIUS servers. See "Configuring WPA-802.1x." |

# Manually Configuring Your Wireless Security

To set up wireless security, you can either manually configure it in the Wireless Settings screen, or you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security (see "Using Push 'N' Connect (WPS) to Configure Your Wireless Network and Security" on page 2-16).

**Note:** If you use a wireless computer to configure wireless security settings, you will be disconnected when you click **Apply**. Reconfigure your wireless computer to match the new settings, or access the modem router from a wired computer to make further changes.

## Restricting Wireless Access to Your Network

By default, any wireless PC that is configured with the correct SSID can access your wireless network. For increased security, the modem router provides several ways to restrict wireless access to your network.

You can do the following:

- Turn off wireless connectivity completely.
- Restrict access based on the wireless network name (SSID).
- Restrict access based on the Wireless Card Access List.

These options are discussed in the following sections.

### Turning off wireless connectivity completely

You can completely turn off the wireless connectivity of the modem router by pressing the Wireless On/Off button on the side panel of the modem router. For example, if you use your notebook computer to wirelessly connect to your modem router and you take a business trip, you can turn off the wireless portion of the modem router while you are traveling. Other members of your household who use computers connected to the modem router through Ethernet cables can still use the modem router. To do this, clear the **Enable Wireless Access Point** check box on the Wireless Settings screen, and then click **Apply**.

### Hiding your wireless network name (SSID)

By default, the modem router is set to broadcast its wireless network name (SSID). You can restrict wireless access to your network by not broadcasting the wireless network name (SSID). To do this, clear the **Allow Broadcast of Name (SSID)** check box on the Wireless Settings screen, and then click **Apply**. Wireless devices will not “see” your modem router. You must configure your wireless devices to match the wireless network name (SSID) of the modem router.

**Warning:** The SSID of any wireless access adapters must match the SSID you specify in the modem router. If they do not match, you will not get a wireless connection to the modem router.

### Restricting access by MAC address

For increased security, you can restrict access to the wireless network to allow only specific PCs based on their MAC addresses. You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the Amodem router. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.The Wireless Station Access list determines which wireless hardware devices will be allowed to connect to the modem router.

To restrict access based on MAC addresses:

1. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.

> **Note:** If you configure the modem router from a wireless computer, add your computer's MAC address to the access list. Otherwise you will lose your wireless connection when you click Apply. You must then access the modem router from a wired computer, or from a wireless computer that is on the access control list, to make any further changes.

2. In the Wireless Settings screen, under the Wireless Station Access List section, click the **Setup Access List** button to display the list.

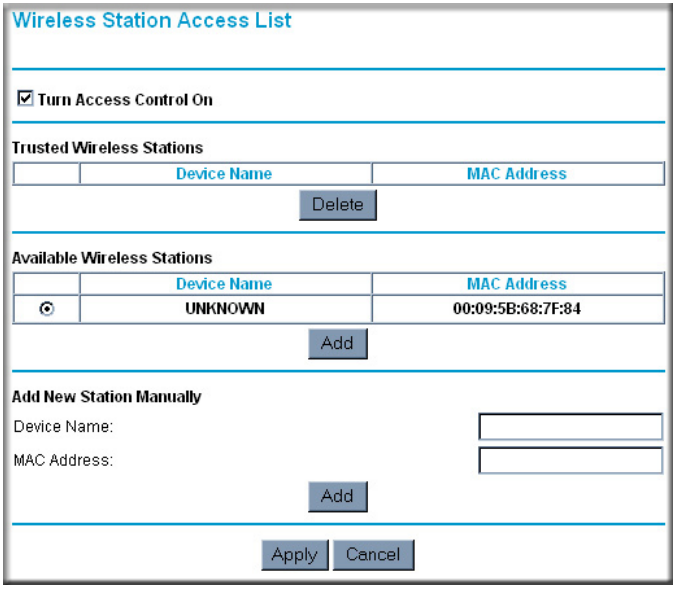



**Figure 2-3**

3. Select the **Turn Access Control On** check box to enable the restricting of wireless computers by their MAC addresses.
4. If the wireless station is currently connected to the network, you can select it from the Available Wireless Stations list. Click **Add** to add the station to the Trusted Wireless Stations list.

5. If the wireless station is not currently connected, you can enter its address manually. Enter the MAC address of the authorized computer. The MAC address is usually printed on the wireless card, or it might appear in the modem router's DHCP table. The MAC address is 12 hexadecimal digits.

   Click **Add** to add your entry. You can add several stations to the list. When you are finished adding stations, click **Apply**.

| | |
|---|---|
| | **Note:** You can copy and paste the MAC addresses from the modem router's Attached Devices screen into the MAC Address field of this screen. To do this, configure each wireless computer to obtain a wireless link to the modem router. The computer should then appear in the Attached Devices screen. |

| | |
|---|---|
| | **Note:** If you are configuring the modem router from a wireless computer whose MAC address is not in the Trusted Wireless Stations list, and you select trusted wireless stations only, you will lose your wireless connection when you click **Apply**. You must then access the modem router from a wired computer to make any further changes. |

6. Make sure the **Turn Access Control On** check box is selected, and then click **Apply**.

Now, only devices on this list will be allowed to wirelessly connect to the modem router. This prevents unauthorized access to your network.

## Configuring Mixed WPA-PSK+WPA2-PSK Security

A high-performance client such as the NETGEAR WN511B must connect to the modem router using WPA2-PSK to achieve maximum performance. Wireless clients that connect to the modem router using WPA-PSK run at no more than 802.11g speed. This option allows wireless clients to use either encryption method.

| | |
|---|---|
| | **Note:** Not all wireless adapters support WPA or WPA2. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings. |

To configure Mixed WPA-PSK+WPA2-PSK:

1. Log in at the default LAN address of **http://192.168.0.1**, with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Select **Wireless Settings** below Setup in the main menu of the modem router.
3. Select the **Mixed WPA-PSK+WPA2-PSK** radio button. The Wireless Settings screen expands to include the WPA-PSK.
4. Enter the pre-shared key in the **Network Key** field using between 8 and 63 characters.

   Click **Save** to save your settings or click **Apply** to allow your changes to take effect immediately.

**Note:** The procedures to configure WPA-PSK and WPA2-PSK are identical to the procedure to configure Mixed WPA-PSK+WPA2-PSK. The only difference is that you select either the **WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)** or **WPA2-PSK (Wi-Fi Protected Access 2 with Pre-Shared Key)** radio button in step 3.

For details about WPA-802.1x authentication options, see "Configuring WPA-802.1x" on page 2-15.

## Choosing Alternative Authentication and Encryption Methods

Restricting wireless access prevents intruders from connecting to your network. However, the wireless data transmissions are still vulnerable to snooping. Using the data encryption settings described in this section will prevent a determined intruder from eavesdropping on your wireless data communications. Also, if you are using the Internet for such activities as purchases or banking, those Internet sites use another level of highly secure encryption called SSL. You can tell if a web site is using SSL because the Web address begins with HTTPS rather than HTTP.

### Configuring WEP

Wired Equivalent Privacy (WEP) security is the most basic and simplest form of wireless security. It is the most often used, but least secure of the available options. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK.

To configure WEP data encryption:

1. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Select **Wireless Settings** in the main menu.
3. In the Security Options section of the screen, select **WEP (Wired Equivalent Privacy)**. The WEP Security Encryption section displays.

**Figure 2-4**

4. Select the authentication type:
   - **Automatic**.This is the default setting.
   - **Open System**.
   - **Shared Key**.
5. Select the encryption strength setting:
   - **64-bit WEP**.
   - **128-bit WEP**.
6. Enter the encryption keys. You can manually or automatically program the four data encryption keys. These values must be identical on all computers and access points in your network.

- Automatic. Enter a word or group of printable characters in the **Passphrase** field and click **Generate**. The four key boxes are automatically populated with key values.
- Manual. The number of hexadecimal digits that you must enter depends on the encryption strength setting:
  - For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).
  - For 128-bit WEP, enter 26 hexadecimal digits (any combination of 0–9, a–f, or A–F).

7. Select the radio button for the key you want to make active.

   Be sure that you clearly understand how the WEP key settings are configured in your wireless adapter. Wireless adapter configuration utilities such as the one included in Windows XP allow entry of only one key, which must match the default key you set in the modem router.

8. Click **Save** to save your settings or click **Apply** to allow your changes to take effect immediately.

| | |
|---|---|
| | **Note:** When configuring the modem router from a wireless computer, if you specify WEP settings, you will lose your wireless connection when you click **Apply**. You must then either configure your wireless adapter to match the modem router WEP settings or access the modem router from a wired computer to make any further changes. |

### Configuring WPA-802.1x

This version of WPA requires the use of a RADIUS server for authentication. Each user (wireless client) must have a user login on the RADIUS server, and the modem router must have a client login on the RADIUS server. Data transmissions are encrypted using a key that is automatically generated.

1. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Select **Wireless Settings** in the main menu.
3. In the Security Options section of the screen, select **WPA-802.1x**.
4. In the **Radius Server Name/IP Address** field, enter the name or IP address of the RADIUS server on your LAN. This is a required field.
5. In the **Radius Port** field, enter the port number used for connections to the RADIUS server. The default port is 1812.

6. In the **Shared Key** field, enter the value that you want to use for the RADIUS shared key. This key enables the modem router to log in to the RADIUS server and must match the client login value used on the RADIUS server.

## Using Push 'N' Connect (WPS) to Configure Your Wireless Network and Security

If your wireless clients support Wi-Fi Protected Setup (WPS), you can use this feature to configure the modem router's SSID and security settings and, at the same time, connect the wireless client securely and easily to the modem router. Look for the symbol on your client device[1] (computers that will connect wirelessly to the modem router are clients). WPS automatically configures the SSID and wireless security settings for the modem router (if the modem router is in its default state) and broadcasts these settings to the wireless client.

Some considerations regarding WPS are:

- WPS supports only WPA-PSK and WPA2-PSK wireless security. WEP security is not supported by WPS.
- NETGEAR's Push 'N' Connect feature is based on the Wi-Fi Protected Setup (WPS) standard. All other Wi-Fi-certified and WPS-capable products should be compatible with NETGEAR products that implement Push 'N' Connect.
- If your wireless network will include a combination of WPS capable devices and non-WPS capable devices, NETGEAR suggests that you set up your wireless network and security settings manually first, and use WPS only for adding additional WPS capable devices. See "Connecting Additional Wireless Client Devices After WPS Setup" on page 2-19.
- If the modem router has already been configured manually, and either WPS-PSK or WPA2-PSK security has been enabled, a wireless client can be connected quickly and simply by using the WPS method of connecting to the wireless network. In this case, the existing wireless settings are broadcast to the WPS-capable client.

These instructions assume that you are configuring WPS on the modem router for the first time and connecting a WPS-capable device.

1. For a list of other Wi-Fi-certified products available from NETGEAR, go to *http://www.wi-fi.org*.

To set up basic wireless connectivity:

1. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.

   You can also enter either of these addresses to connect to the modem router: **http://www.routerlogin.net** or **http://www.routerlogin.com**.

2. Select Add WPS Client (computers that will connect wirelessly to the router are clients) in the main menu. The Add WPS Client wizard screen displays.

   **Note:** If you cannot select Add WPS Client, check to see if WPS is disabled in the Advanced Wireless Settings screen. See "Using Static Routes" on page 5-12.

3. Click **Next.** The screen changes to allow you to select the method for adding the WPS client.
4. Select the method for adding the WPS client. A WPS client can be added using the Push Button method or the PIN method.
   - **Using the Push Button**. This is the preferred method. (See Figure 2-5 on page 2-17.)
     - Select the **Push Button** radio box and either press the WPS Push Button on the side of the modem router or click the soft WPS Push Button on the screen (as shown below).
     - The modem router will attempt to communicate with the client; you have 2 minutes to enable WPS from the client device using the client's WPS networking utility.

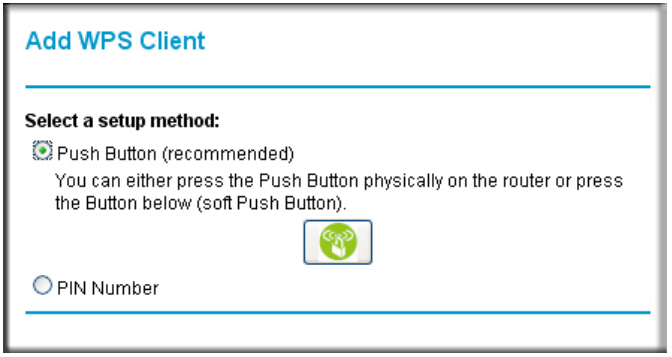

Add WPS Client
Select a setup method:
Push Button (recommended)
You can either press the Push Button physically on the router or press the Button below (soft Push Button).
PIN Number

**Figure 2-5**

- **Entering a PIN**. If you want to use the PIN method, select the **PIN** radio box. A screen similar to the one shown below displays.
  - Go to your wireless client and, from the client's WPS utility, obtain the wireless client's security PIN, or follow the client's WPS utility instructions to generate a security PIN.
  - Then, enter this PIN in the **Enter Client's PIN** field provided on the modem router and click **Apply**. You have 4 minutes to enable WPS on the router using this method.

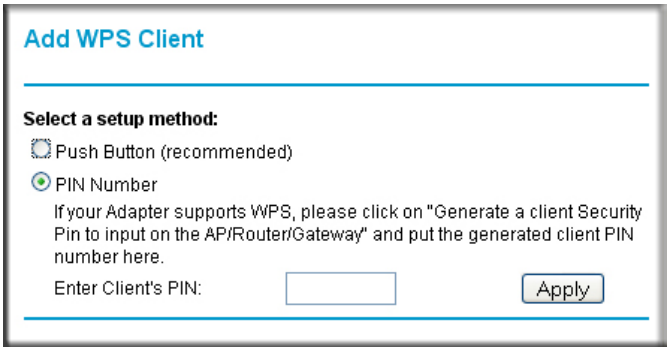

Add WPS Client
Select a setup method:
Push Button (recommended)
PIN Number
If your Adapter supports WPS, please click on "Generate a client Security Pin to input on the AP/Router/Gateway" and put the generated client PIN number here.
Enter Client's PIN:
Apply

**Figure 2-6**

Using either method, the client wireless device will attempt to detect the WPS signal from the modem router and establish a wireless connection in the time allotted.

- While the modem router attempts to connect to a WPS-capable device, the Push 'N' Connect LED on the front of the modem router blinks green. When the modem router has established a WPS connection, the LED is solid green.
- If a connection is established, the modem router WPS screen displays a message confirming that the wireless client was successfully added to the wireless network. (The modem router has generated an SSID, implemented WPA/WPA2 wireless security [including a PSK security password] on the modem router, and has sent this configuration to the wireless client.)

**5.** Note the new SSID and WPA/WPA2 password for the wireless network.

To access the Internet from any computer connected to your modem router, launch a browser such as Microsoft Internet Explorer. You should see the modem router's Internet LED blink, indicating communication to the ISP.

**Note:** If no WPS-capable client devices are located during the 2-minute timeframe, security will not be implemented on the modem router.

For more information about WPS, see "Using Static Routes" in Chapter 5.

## Connecting Additional Wireless Client Devices After WPS Setup

You can add more WPS clients to your wireless network, or you can add a combination of WPS-enabled clients and clients without WPS.

**Note:** Your wireless settings remain the same when you add another WPS-enabled client, as long as the **Keep Existing Wireless Settings** checkbox is selected in the Advanced WPS Settings screen (listed under the Advanced heading in the modem router main menu). If you clear this checkbox, when you add the client, a new SSID and passphrase will be generated, and all existing connected wireless clients will be disassociated and disconnected from the modem router.

To add a wireless client device that is WPS-enabled:

1. Follow the procedures in "Using Push 'N' Connect (WPS) to Configure Your Wireless Network and Security" on page 2-16.
2. To view a list of all devices connected to your modem router (including wireless and Ethernet-connected), see "Viewing Attached Devices" in Chapter 4.

For non-WPS clients, you cannot use the WPS setup procedures to add them to the wireless network. You must record, and then manually enter your security settings (see "Manually Configuring Your Wireless Security" on page 2-9).

To connect a combination of non-WPS enabled and WPS-Enabled clients to the modem router:

1. Restore the modem router to its factory default settings (press both the Wireless and WPS buttons on the side of the modem router for 5 seconds).

   When the factory settings are restored, all existing wireless clients are disassociated and disconnected from the modem router.

2. Configure the network names (SSIDs), select the WPA/PSK + WPA2/PSK radio button on the Wireless Settings screen (see "Manually Configuring Your Wireless Security" on page 2-9) and click **Apply**. On the WPA/PSK + WPA2/PSK screen, select a passphrase and click **Apply**. Record this information to add additional clients.
3. For the non-WPS devices that you want to connect, open the networking utility and follow the utility's instructions to enter the security settings that you selected in step 2 (the SSID, WPA/PSK + WPA2/PSK security method, and passphrase).
4. For the WPS devices that you want to connect, follow the procedures in "Using Push 'N' Connect (WPS) to Configure Your Wireless Network and Security" on page 2-16.

   The settings that you configured in Step 2 are broadcast to the WPS devices so that they can connect to the modem router.

**Note:** To make sure that your new wireless settings remain in effect, verify that the **Keep Existing Wireless Settings** checkbox is selected in the Advanced WPS Settings screen.

To view a list of all devices connected to your modem router (including wireless- and Ethernet-connected), see "Viewing Attached Devices" in Chapter 4.

# Chapter 3
# Protecting Your Network

This chapter describes how to use the basic firewall features of the modem router to protect your network. This chapter includes:


- "Protecting Access to Your Modem Router"
- "Blocking Keywords, Sites, and Services" on page 3-3"
- "Firewall Rules" on page 3-5"
- "Services" on page 3-12"
- "Setting Times and Scheduling Firewall Services" on page 3-13"


## Protecting Access to Your Modem Router

For security reasons, the modem router has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login automatically disconnects. When prompted, enter **admin** for the modem router user name and **password** for the modem router password. You can use the following procedures to change the modem router's password and the period for the administrator's login time-out.

| | |
|---|---|
| | **Note:** The user name and password are not the same as any other user name or password your might use to log in to your Internet connection. |

NETGEAR recommends that you change this password to a more secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of both upper case and lower case letters, numbers, and symbols. Your password can be up to 30 characters.

## Changing the Built-In Password

1. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever password and LAN address you have chosen for the modem router.

**Figure 3-1**

2. In the main menu, under Maintenance, select **Set Password** to display the following screen:

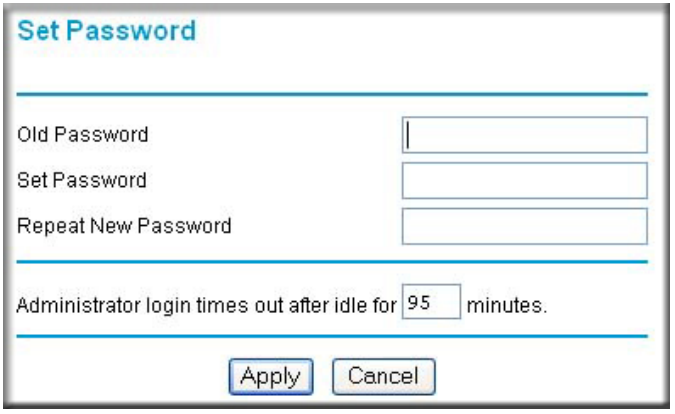



**Figure 3-2**

3. To change the password, first enter the old password, and then enter the new password twice.
4. Click **Apply** to save your changes.

| | |
|---|---|
| | **Note:** After changing the password, you are required to log in again to continue the configuration. If you have backed up the modem router settings previously, you should do a new backup so that the saved settings file includes the new password. |

## Changing the Administrator Login Time-out

For security, the administrator's login to the modem router configuration times out after a period of inactivity. To change the login time-out period:

1. In the Set Password screen, type a number in the **Administrator login times** out field. The suggested default value is 5 minutes.
2. Click **Apply** to save your changes, or click **Cancel** to keep the current period.

# Blocking Keywords, Sites, and Services

The modem router provides a variety of options for blocking Internet-based content and communications services. With its content filtering feature, the modem router prevents objectionable content from reaching your PCs. The modem router allows you to control access to Internet content by screening for keywords within Web addresses. Key content filtering options include:

- Keyword blocking of HTTP traffic.
- Outbound service blocking. Limits access from your LAN to Internet locations or services that you specify as off-limits.
- Denial of service (DoS) protection. Automatically detects and thwarts denial of service (DoS) attacks such as Ping of Death, SYN flood, LAND Attack, and IP spoofing.
- Blocking unwanted traffic from the Internet to your LAN.

To block keywords and sites:

1. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever password and LAN address you might have previously set for the modem router.
2. In the main menu, under Security, select **Block Sites** to display the following screen

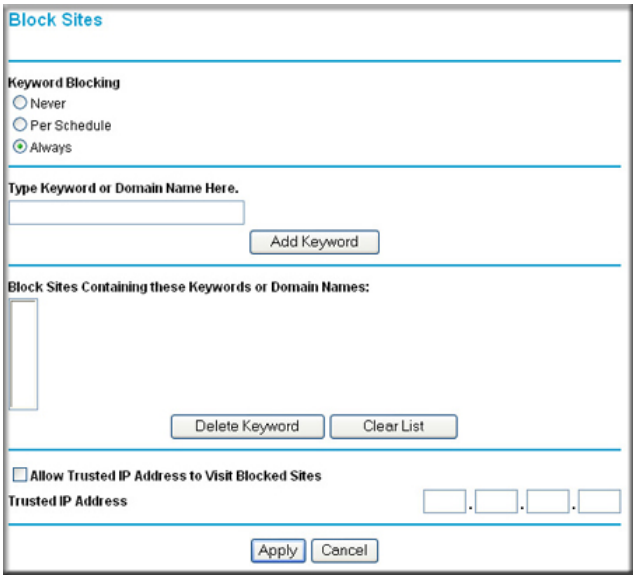



**Figure 3-3**

3. To enable keyword blocking, select one of the following:
   - **Per Schedule**. Turn on keyword blocking according to the settings in the Schedule screen.
   - **Always**. Turn on keyword blocking all the time, independent of the Schedule screen.
4. Enter a keyword or domain in the **Keyword** field, click **Add Keyword**, and then click **Apply**.

   Some examples of keyword application follow:
   - If the keyword XXX is specified, the URL http://www.badstuff.com/xxx.html is blocked.
   - If the keyword .com is specified, only websites with other domain suffixes (such as .edu or .gov) can be viewed.
   - Enter a period (**.**) as to block all Internet browsing access.

   Up to 32 entries are supported in the Keyword list.
5. To delete a keyword or domain, select it from the list, click **Delete Keyword**, and then click **Apply**.
6. To specify a trusted user, enter that computer's IP address in the **Trusted IP Address** field, and click **Apply**.

You can specify one trusted user, which is a computer that will be exempt from blocking and logging. Since the trusted user will be identified by an IP address, you should configure that computer with a fixed IP address.

7. Click **Apply** to save your settings.

## Firewall Rules

Firewall rules block or allow specific traffic passing through from one side of the router to the other. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what outside resources local users can have access to.

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the modem router are:

- **Inbound**. Block all access from outside except responses to requests from the LAN side.
- **Outbound**. Allow all access from the LAN side to the outside.

You can define additional rules that will specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. You can also choose to log traffic that matches or does not match the rule you have defined.

You can change the order of precedence of rules so that the rule that applies most often takes effect first. See “Order of Precedence for Rules” on page 3-11 for more details.

To access the rules configuration of the modem router, select **Firewall Rules** on the main menu, and then click **Add** for either an outbound or inbound service. The Firewall Rules screen displays.

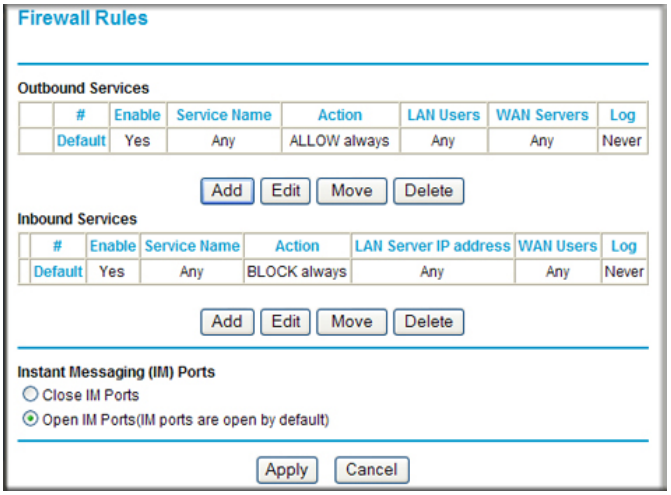

Firewall Rules
Outbound Services
# Enable Service Name Action LAN Users WAN Servers Log
Default Yes Any ALLOW always Any Any Never
Add Edit Move Delete
Inbound Services
# Enable Service Name Action LAN Server IP address WAN Users Log
Default Yes Any BLOCK always Any Any Never
Add Edit Move Delete
Instant Messaging (IM) Ports
Close IM Ports
Open IM Ports(IM ports are open by default)
Apply Cancel

**Figure 3-4**

- To edit an existing rule, select its button on the left side of the table, and click **Edit**.
- To delete an existing rule, select its button on the left side of the table, and click **Delete**.
- To move an existing rule to a different position in the table, select its button on the left side of the table, and click **Move**. At the prompt, enter the number of the desired new position and click **OK**.

## Inbound Rules (Port Forwarding)

Because the modem router uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a Web server or game server) visible and available to the Internet. The rule tells the modem router to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding.

| | |
|---|---|
| | **Note:** Some residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP might periodically check for servers and might suspend your account if it discovers any active services at your location. If you are unsure, refer to the acceptable use policy of your ISP. |

Remember that allowing inbound services opens holes in your firewall. Enable only those ports that are necessary for your network. Following are two application examples of inbound rules.

### Inbound Rule Example: A Local Public Web Server

If you host a public Web server on your local network, you can define a rule to allow inbound Web (HTTP) requests from any outside IP address to the IP address of your Web server at any time of day. This rule is shown in the following figure:

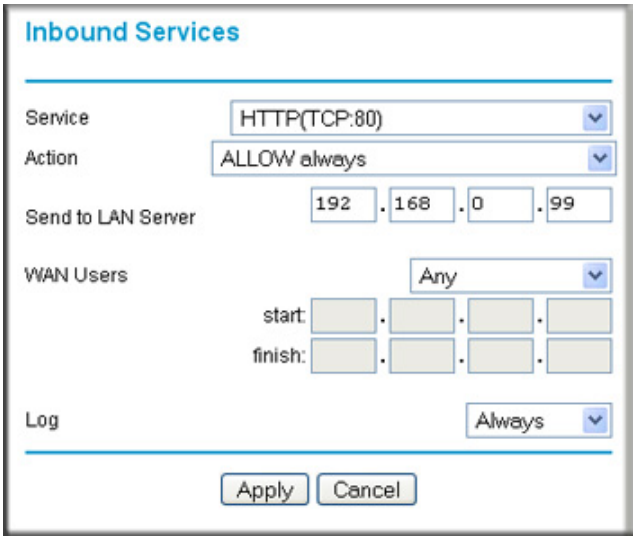



**Figure 3-5**

The settings are:

- **Service**. From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Services screen to add any additional services or applications that do not already appear. See "To define services:" on page 3-12.
- **Action**. Choose how you want this type of traffic to be handled. You can block or allow always, or you can block or allow according to the schedule you have defined in the Schedule screen.
- **Send to LAN Server**. Enter the IP address of the computer or server on your LAN that will receive the inbound traffic covered by this rule.

- **WAN Users**. These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the option that you want:
  - **Any**: All IP addresses are covered by this rule.
  - **Address range**: If this option is selected, you must fill in the **Start** and **Finish** fields.
  - **Single address**: Enter the required address in the **Start** field.
- **Log**. You can select whether the traffic will be logged. The choices are:
  - **Never**. No log entries will be made for this service.
  - **Always**. Any traffic for this service type will be logged.
  - **Match**. Traffic of this type that matches the settings and action will be logged.
  - **Not match**. Traffic of this type that does not match the settings and action will be logged.

### Inbound Rule Example: Allowing Video conferencing

If you want to allow incoming video conferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office, you can create an inbound rule. In the example shown in the following figure, CU-SeeMe connections are allowed only from a specified range of external IP addresses. In this case, we have also specified logging of any incoming CU-SeeMe requests that do not match the allowed settings.

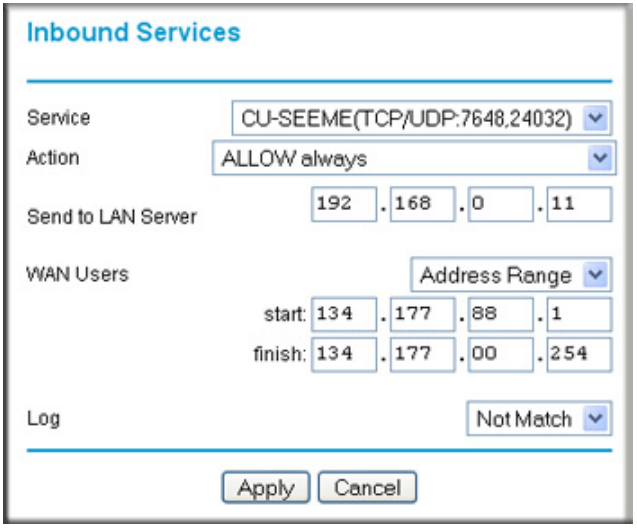



**Figure 3-6**

### Considerations for Inbound Rules

- If your external IP address is assigned dynamically by your ISP, the IP address might change periodically as the DHCP lease expires. Consider using the Dynamic DNS screen so that external users can always find your network.
- If the IP address of the local server computer is assigned by DHCP, it might change when the computer is rebooted. To avoid this, use the Reserved IP address feature in the LAN IP Setup screen to keep the computer's IP address constant.
- Local computers must access the local server using the computer's local LAN address (192.168.0.11 in the example in the previous figure). Attempts by local computers to access the server using the external WAN IP address will fail.

## Outbound Rules (Service Blocking)

The modem router allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. You can define an outbound rule to block Internet access from a local computer based on the following:

- IP address of the local computer (source address)
- IP address of the Internet site being contacted (destination address)
- Time of day
- Type of service being requested (service port number)

Following is an application example of outbound rules.

### Outbound Rule Example: Blocking Instant Messenger

If you want to block Instant Messenger usage by employees during working hours, you can create an outbound rule to block that application from any internal IP address to any external address according to the schedule that you create in the Schedule screen.You can specify that the modem router logs any attempt to use Instant Messenger during this blocked period. You can also open or close AOL or MSN Instant Messenger ports: see the Firewall Rules screen in the "Order of Precedence for Rules" section on page 3-11.

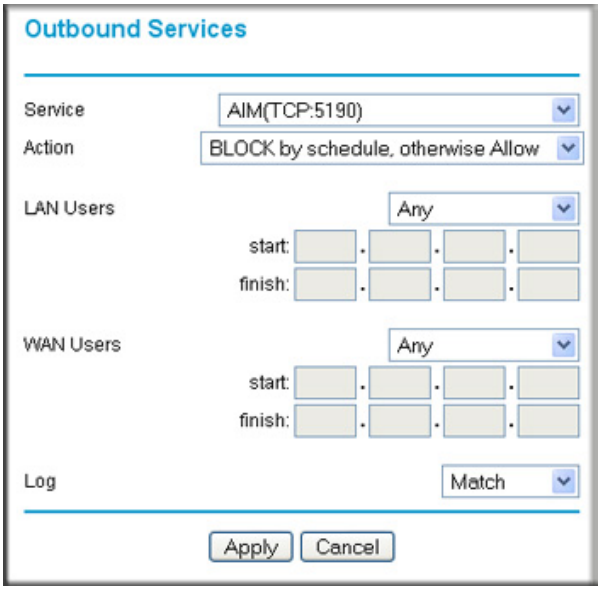



**Figure 3-7**

The settings are:

- **Service**. From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the **Add Custom Service** button in the Services screen to add any additional services or applications that do not already appear.
- **Action**. Choose how you want this type of traffic to be handled. You can block or allow always, or you can block or allow according to the schedule you have defined in the Schedule screen.
- **LAN Users**. These settings determine which packets are covered by the rule, based on their source LAN IP address. Select the option that you want:
  - **Any**. All IP addresses are covered by this rule.
  - **Address range**. If this option is selected, you must fill in the **Start** and **Finish** fields.
  - **Single address**. Enter the required address in the **Start** field.
- **WAN Users**. These settings determine which packets are covered by the rule, based on their destination WAN IP address. Select the option that you want:
  - **Any**. All IP addresses are covered by this rule.
  - **Address range**. If this option is selected, you must fill in the **Start** and **Finish** fields.

  - **Single address**. Enter the required address in the **Start** field.

- **Log**. You can select whether the traffic will be logged. The choices are:
  - **Never**. No log entries will be made for this service.
  - **Always**. Any traffic for this service type will be logged.
  - **Match**. Traffic of this type that matches the settings and action will be logged.
  - **Not match**. Traffic of this type that does not match the settings and action will be logged.

## Order of Precedence for Rules

As you define new rules, they are added to the tables in the Firewall Rules screen, as shown in the following figure:

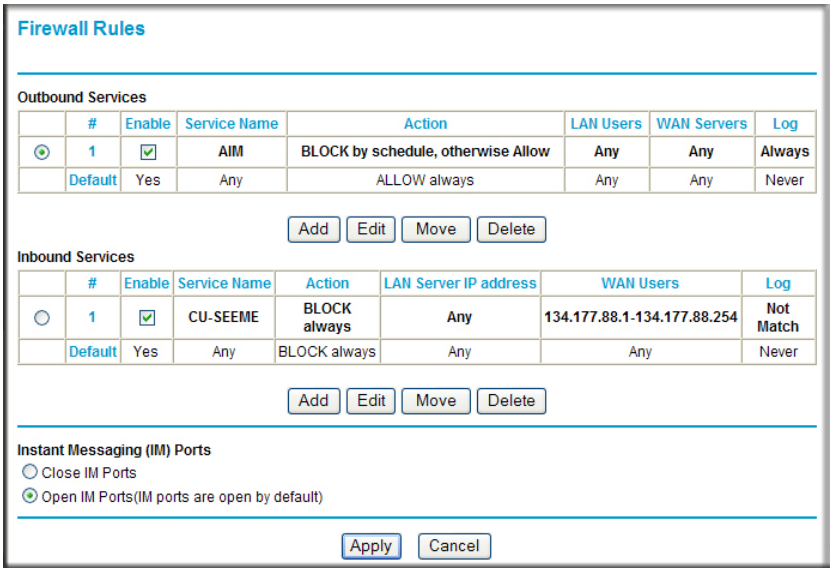

Firewall Rules
Outbound Services
# Enable Service Name Action LAN Users WAN Servers Log
1 AIM BLOCK by schedule, otherwise Allow Any Any Always
Default Yes Any ALLOW always Any Any Never
Add Edit Move Delete
Inbound Services
# Enable Service Name Action LAN Server IP address WAN Users Log
1 CU-SEEME BLOCK always Any 134.177.88.1-134.177.88.254 Not Match
Default Yes Any BLOCK always Any Any Never
Add Edit Move Delete
Instant Messaging (IM) Ports
Close IM Ports
Open IM Ports(IM ports are open by default)
Apply Cancel

**Figure 3-8**

For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the Rules table, beginning at the top and proceeding to the default rules at the bottom. In some cases, the order of precedence of two or more rules might be important in determining the disposition of a packet. The **Move** button allows you to relocate a defined rule to a new position in the table.

To easily open or close AOL or MSN Instant Messenger ports:

1. Under Instant Messaging (IM) Ports, select a radio button:
   - **Close IM Ports**. Specifies to disable instant messaging traffic.
   - **Open IM Ports**. Specifies to enable instant messaging traffic. IM ports are open by default.
2. Click **Apply** to save your changes.

## Services

Services are functions performed by server computers at the request of client computers. For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (Web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application.

Although the modem router already holds a list of many service port numbers, you are not limited to these choices. Use the following procedure to create your own service definitions.

To define services:

1. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin**, and default password of **password**, or using whatever password and LAN address you have chosen for the modem router.
2. Select Services below Security to display the Services screen shown in the following figure:

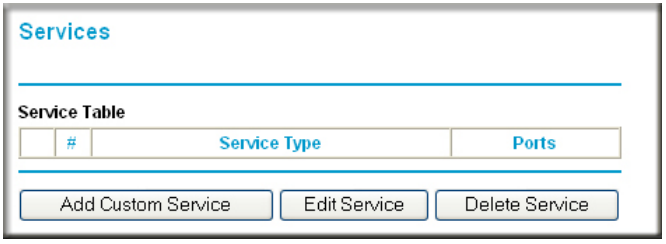



**Figure 3-9**

- To create a new service, click the **Add Custom Service** button.
- To edit an existing service, select its button on the left side of the table, and click **Edit Service**.
- To delete an existing service, select its button on the left side of the table, and click **Delete Service**.

3. Use the screen shown here to define or edit a service.

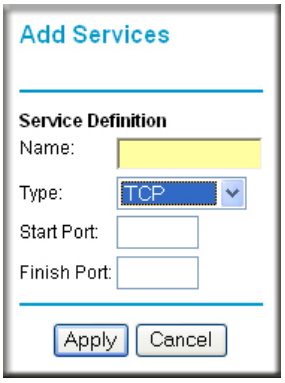



**Figure 3-10**

4. Click **Apply** to save your changes.

# Setting Times and Scheduling Firewall Services

The modem router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet.

## Setting Your Time Zone

To localize the time for your log entries, you must specify your time zone:

1. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever password and LAN address you have chosen for the modem router.

2. Click **Schedule** below Security to display the Schedule screen.

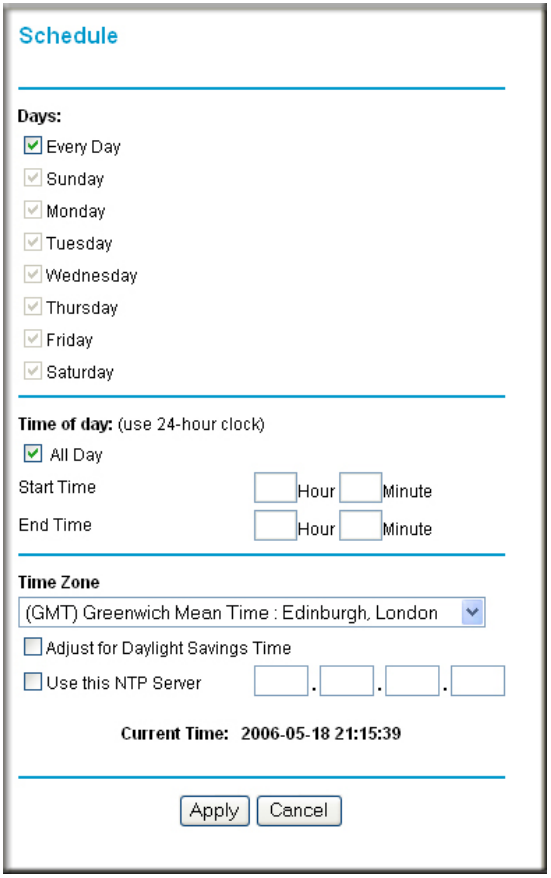



**Figure 3-11**

3. Select your time zone. This setting is used for the blocking schedule according to your local time zone and for time-stamping log entries.

   Select the **Adjust for Daylight Savings Time** check box if your time zone is currently in daylight savings time.

| | |
|---|---|
| | **Note:** If your region uses daylight savings time, you must manually select Adjust for Daylight Savings Time on the first day of daylight savings time, and clear it at the end. Enabling daylight savings time causes one hour to be added to the standard time. |

4. The modem router has a list of NETGEAR NTP servers. If you would prefer to use a particular NTP server as the primary server, select the **Use this NTP Server** check box, and enter its IP address.
5. Click **Apply** to save your settings.

## Scheduling Firewall Services

If you enabled services blocking in the Block Services screen or port forwarding in the Ports screen, you can set up a schedule for when blocking occurs or when access is not restricted.

1. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever password and LAN address you have chosen for the modem router.
2. Select Schedule below Security to display the Schedule screen that is shown in Figure 3-11.
3. To block Internet services based on a schedule, select **Every Day** or select one or more days. If you want to limit access completely for the selected days, select **All Day**. Otherwise, to limit access during certain times for the selected days, or enter times in the **Start Time** and **End Time** fields.

**Note:** Enter the values in 24-hour time format. For example, 10:30 a.m. would be 10 hours and 30 minutes, and 10:30 p.m. would be 22 hours and 30 minutes. If you set the start time after the end time, the schedule will be effective through midnight the next day.

4. Click **Apply** to save your changes.

# Chapter 4
# Managing Your Network

This chapter describes how to perform network management tasks with your DGN2000 Wireless-N ADSL2+ Modem Router. This chapter includes:


- "Backing Up, Restoring, and Erasing Your Settings"
- "Upgrading the Modem Router Firmware" on page 4-3"
- "Network Management Information" on page 4-4"
- "Enabling Security Event E-mail Notification" on page 4-13"
- "Running Diagnostic Utilities and Rebooting the Modem Router" on page 4-14"
- "Configuring Remote Management" on page 4-15"
- "Automatic Firmware Recovery" on page 4-17"


## Backing Up, Restoring, and Erasing Your Settings

The configuration settings of the modem router are stored in a configuration file. This file can be backed up to your computer, restored, or reverted to factory default settings. The following procedures explains how to do these tasks.

### Backing Up the Configuration to a File

1. Log in to the modem routeras at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever user name, password, and LAN address you have chosen for the modem router.
2. In the main menu, below Maintenance, select Backup Settings to display the following screen.

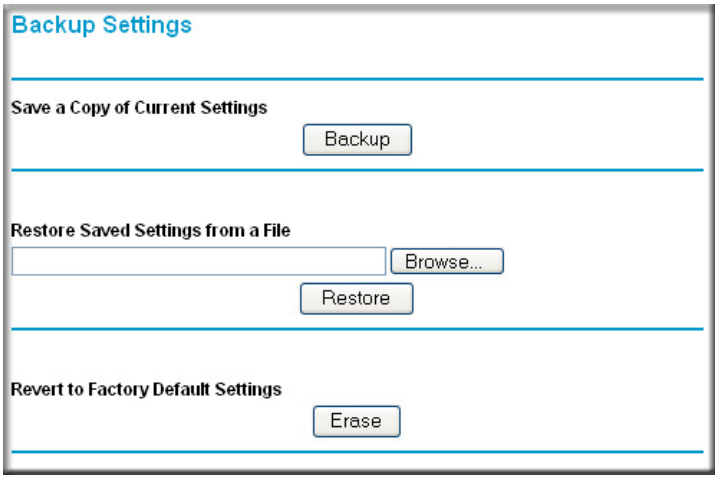



**Figure 4-1**

3. Click **Backup** to save a copy of the current settings.
4. Store the .cfg file on a computer on your network.

## Restoring the Configuration from a File

1. Log in to the modem router as described in "Logging In to the Modem Router" on page 1-2.
2. In the main menu, below Maintenance, select Backup Settings as shown in Figure 4-1.
3. Enter the full path to the file on your network, or click the **Browse** button to locate the file.
4. When you have located the .cfg file, click the **Restore** button to upload the file to the modem router.
5. The modem router then reboots automatically.

## Erasing the Configuration

Sometimes you might want to restore the modem router to the factory default settings. This can be done by using the erase function.

1. To erase the configuration, select Backup Settings under Maintenance in the main menu, and click the **Erase** button on the screen.
2. The modem router then reboots automatically.

After an erase, the modem router's password is **password**, the LAN IP address is **192.168.0.1**, and the modem router's DHCP client is enabled.

**Note:** To restore the factory default configuration settings when you do not know the login password or IP address, press the Wireless On/Off and WPS buttons on the side panel of the modem router simultaneously for 6 seconds.

## Upgrading the Modem Router Firmware

The software of the modem router is stored in flash memory, and can be upgraded as NETGEAR releases new software. Upgrade files can be downloaded from NETGEAR's website. If the upgrade file is compressed (.zip file), you must first extract the binary (.bin or .img) file before uploading it to the modem router.

**Note:** NETGEAR recommends that you back up your configuration before doing a firmware upgrade. After the upgrade is complete, you might need to restore your configuration settings.

To upgrade the firmware:

1. Download and unzip the new software file from NETGEAR.

   The Web browser used to upload new firmware into the modem router must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer 5.0 or later.

2. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever user name, password, and LAN address you have chosen for the modem router.

3. In the main menu, under Maintenance, select Router Upgrade to display the Firmware Upgrade screen.

**Figure 4-2**

4. In the Firmware Upgrade screen, click **Browse** to locate the binary (.bin or .img) upgrade file.
5. Click **Upload**.

| | |
|---|---|
| | **Note:** When uploading software to the modem router, do not interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it might corrupt the software. When the upload is complete, your modem router automatically restarts. The upgrade process typically takes about one minute. In some cases, you might need to clear the configuration and reconfigure the modem router after upgrading. |

# Network Management Information

The modem router provides a variety of status and usage information, which is discussed in the following sections.

## Viewing the Modem Router Status and Usage Statistics

In the main menu, under Maintenance, select Router Status to display the Router Status screen (Figure 4-3, upper part and Figure 4-4, lower part):

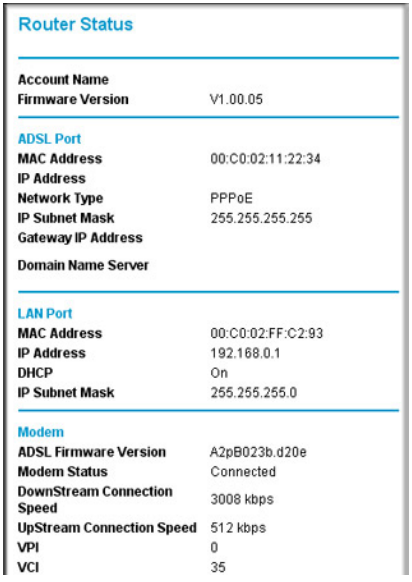



**Figure 4-3**

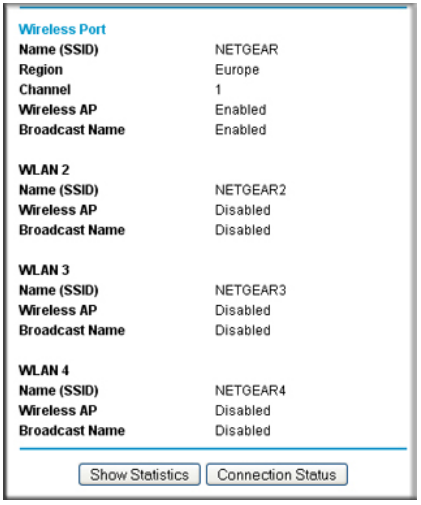



**Figure 4-4**

The Router Status screen provides status and usage information, including the following settings.

**Table 4-1. Router Status Fields**

| Component | Field | Description |
|---|---|---|
| | Account Name | The host name that is assigned to the modem router in the Basic Settings screen. |
| | Firmware Version | This field displays the modem router firmware version. |
| ADSL Port | MAC Address | This field displays the Ethernet MAC address being used by the Internet (ADSL) port of the modem router. |
| | IP Address | This field displays the IP address being used by the Internet (ADSL) port of the modem router. If no address is shown, the modem router cannot connect to the Internet. |
| | Network Type | The network type depends upon your ISP. |
| | IP Subnet Mask | This field displays the IP subnet mask being used by the Internet (ADSL) port of the modem router. |
| | Gateway IP Address | IP address used as a gateway to the Internet for computers configured to use DHCP. |
| | Domain Name Server | This field displays the DNS server IP addresses being used by the modem router. These addresses are usually obtained dynamically from the ISP. |

**Table 4-1. Router Status Fields (continued)**

| Component | Field | Description |
|---|---|---|
| LAN Port | MAC Address | This field displays the Ethernet MAC address being used by the local (LAN) port of the modem router. |
| | IP Address | This field displays the IP address being used by the local (LAN) port of the modem router. The default is 192.168.0.1. |
| | DHCP | If Off, the modem router does not assign IP addresses to PCs on the LAN.<br>If On, the modem router does assign IP addresses to PCs on the LAN. |
| | IP Subnet Mask | This field displays the IP subnet mask being used by the local (LAN) port of the modem router. The default is 255.255.255.0. |
| Modem | ADSL Firmware Version | The version of the firmware. |
| | Modem Status | The connection status of the modem. |
| | DownStream Connection Speed | The speed at which the modem is receiving data from the ADSL line. |
| | UpStream Connection Speed | The speed at which the modem is transmitting data to the ADSL line. |
| | VPI | The Virtual Path Identifier setting. |
| | VCI | The Virtual Channel Identifier setting. |
| **Wireless Port** | The wireless port settings are specified in the Wireless Settings screen; see "Manually Configuring Your Wireless Network" in Chapter 2 for details. | |
| WLAN 1 | Name (SSID) | The service set ID, also known as the wireless network name for WLAN1. |
| | Region | The country where the unit is set up for use. |
| | Channel | The current channel, which determines the operating frequency. |
| | Wireless AP | Indicates if the access point feature is enabled for WLAN1. If disabled, the Wireless LED on the front panel is off. |
| | Broadcast Name | Indicates if the modem router is configured to broadcast its SSID for WLAN1. |
| WLAN2 | Name (SSID) | The wireless network name for WLAN2. |
| | Wireless AP | Indicates if the access point feature is enabled for WLAN2. |
| | Broadcast Name | Indicates if the modem router is configured to broadcast its SSID for WLAN2. |

**Table 4-1. Router Status Fields (continued)**

| Component | Field | Description |
|---|---|---|
| WLAN3 | Name (SSID) | The wireless network name for WLAN3. |
| | Wireless AP | Indicates if the access point feature is enabled for WLAN3. |
| | Broadcast Name | Indicates if the modem router is configured to broadcast its SSID for WLAN3. |
| WLAN4 | Name (SSID) | The wireless network name for WLAN4. |
| | Wireless AP | Indicates if the access point feature is enabled for WLAN4. |
| | Broadcast Name | Indicates if the modem router is configured to broadcast its SSID for WLAN4. |

Click the **Show Statistics** button to display modem router usage statistics, as shown in the following screen.

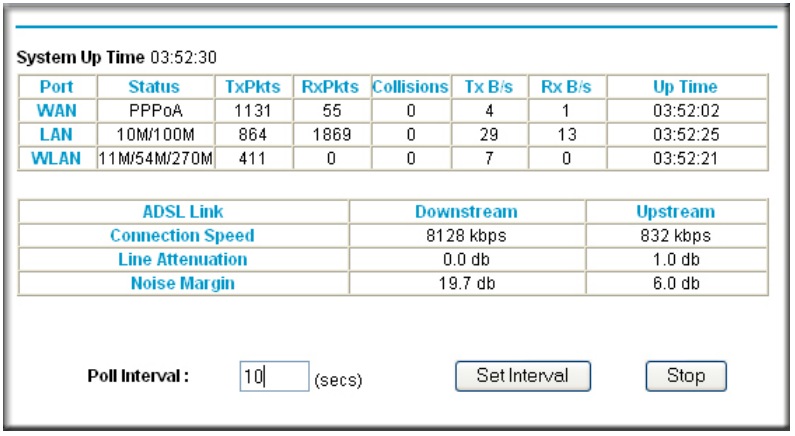

System Up Time 03:52:30
Port Status TxPkts RxPkts Collisions Tx B/s Rx B/s Up Time
WAN PPPoA 1131 55 0 4 1 03:52:02
LAN 10M/100M 864 1869 0 29 13 03:52:25
WLAN 11M/54M/270M 411 0 0 7 0 03:52:21
ADSL Link Downstream Upstream
Connection Speed 8128 kbps 832 kbps
Line Attenuation 0.0 db 1.0 db
Noise Margin 19.7 db 6.0 db
Poll Interval : 10 (secs)
Set Interval
Stop

**Figure 4-5**

This screen shows the following statistics:.

**Table 4-2. Router Statistics Fields**

| Field | Description |
|---|---|
| WAN, LAN, or WLAN | The statistics for the WAN (Internet), LAN (local), and wireless LAN (WLAN) ports. For each port, the screen displays the following: |
| Status | The link status of the port. |
| TxPkts | The number of packets transmitted on this port since reset or manual clear. |

**Table 4-2. Router Statistics Fields (continued)**

| Field | Description |
|---|---|
| RxPkts | The number of packets received on this port since reset or manual clear. |
| Collisions | The number of collisions on this port since reset or manual clear. |
| Tx B/s | The current line utilization—percentage of current bandwidth used on this port. |
| Rx B/s | The average line utilization for this port. |
| Up Time | The time elapsed since the last power cycle or reset. |
| ADSL Link Downstream or Upstream | The statistics for the upstream and downstream ADSL link. These statistics will be of interest to your technical support representative if you are having problems obtaining or maintaining a connection. |
| Connection Speed | Typically, the downstream speed is faster than the upstream speed. |
| Line Attenuation | The line attenuation increases the further you are physically located from your ISP's facilities. |
| Noise Margin | This is the signal-to-noise ratio and is a measure of the quality of the signal on the line. |
| Poll Interval | Specifies the interval at which the statistics are updated in this window. Click **Stop** to freeze the display. |

Click the **Connection Status** button to display modem router connection status, as shown in the following screen.

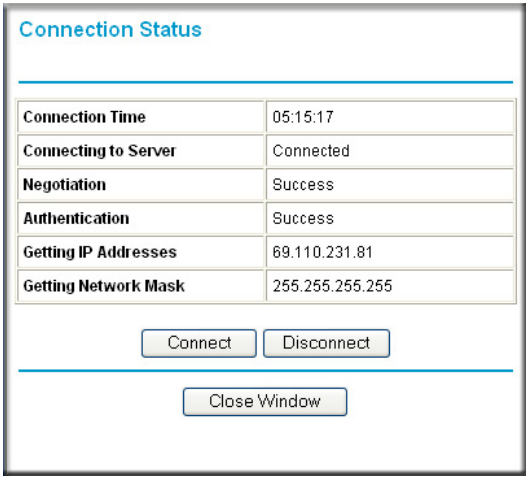



**Figure 4-6**

This screen shows the following statistics:

**Table 4-3. Connection Status Fields (PPPoE Network Type Example)**

| Field | Description |
|---|---|
| Connection Time | The time elapsed since the last connection to the Internet through the ADSL port. |
| Connecting to sender | The connection status. |
| Negotiation | Success or Failed. |
| Authentication | Success or Failed. |
| Obtaining IP Address | The IP address assigned to the WAN port by the ADSL Internet Service Provider. |
| Obtaining Network Mask | The network mask assigned to the WAN port by the ADSL Internet Service Provider. |

## Viewing Attached Devices

The Attached Devices screen contains a table of all IP devices that the modem router has discovered on the local network. In the main menu, under Maintenance, select **Attached Devices** to view the table, shown in the following screen.

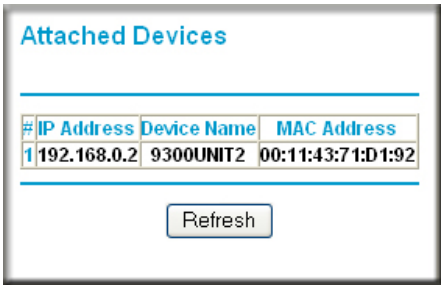



**Figure 4-7**

For each device, the table shows the IP address, device name if available, and the Ethernet MAC address. Note that if the modem router is rebooted, the table data is lost until the modem router rediscovers the devices. To force the modem router to look for attached devices, click the **Refresh** button.

## Viewing, Selecting, and Saving Logged Information

The modem router logs security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enabled content filtering in the Block Sites screen, the Logs screen can show you when someone on your network tries to access a blocked site. If you enabled e-mail notification, you receive these logs in an e-mail message. If you do not have e-mail notification enabled, you can view the logs here.

An example of the logs file is shown in the following screen.

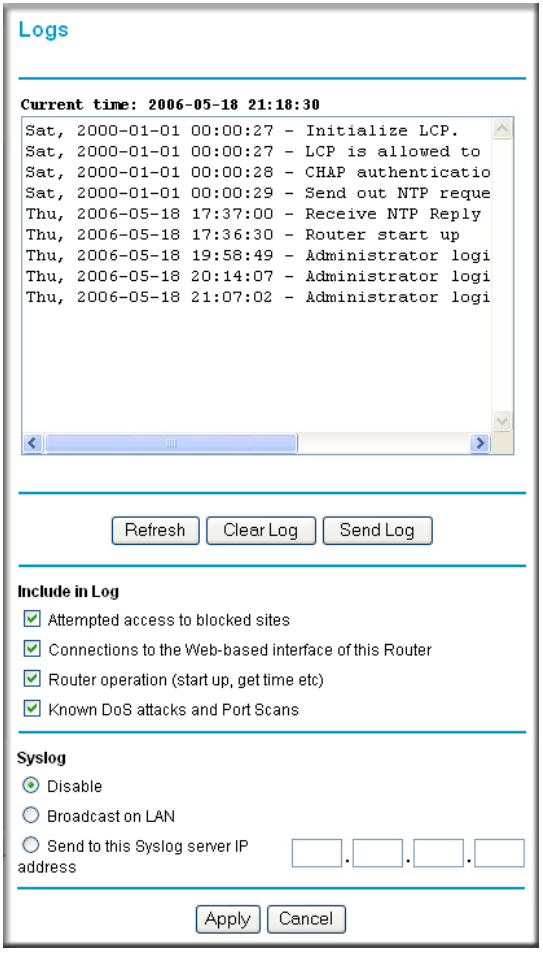

Logs
Current time: 2006-05-18 21:18:30
Sat, 2000-01-01 00:00:27 - Initialize LCP.
Sat, 2000-01-01 00:00:27 - LCP is allowed to
Sat, 2000-01-01 00:00:28 - CHAP authenticatio
Sat, 2000-01-01 00:00:29 - Send out NTP reque
Thu, 2006-05-18 17:37:00 - Receive NTP Reply
Thu, 2006-05-18 17:36:30 - Router start up
Thu, 2006-05-18 19:58:49 - Administrator logi
Thu, 2006-05-18 20:14:07 - Administrator logi
Thu, 2006-05-18 21:07:02 - Administrator logi
Refresh
Clear Log
Send Log
Include in Log
Attempted access to blocked sites
Connections to the Web-based interface of this Router
Router operation (start up, get time etc)
Known DoS attacks and Port Scans
Syslog
Disable
Broadcast on LAN
Send to this Syslog server IP address
Apply
Cancel

**Figure 4-8**

Log entries are described in the following table.

**Table 4-4. Security Log Entry Descriptions**

| Field | Description |
|---|---|
| Date and time | The date and time the log entry was recorded. |
| Description or action | The type of event and what action was taken, if any. |
| Source IP | The IP address of the initiating device for this log entry. |
| Source port and interface | The service port number of the initiating device, and whether it originated from the LAN or WAN. |
| Destination | The name or IP address of the destination device or website. |
| Destination port and interface | The service port number of the destination device, and whether it is on the LAN or WAN. |

Log action buttons are described in the following table.

**Table 4-5. Security Log Action Buttons**

| Field | Description |
|---|---|
| Refresh | Refresh the log screen. |
| Clear Log | Clear the log entries. |
| Send Log | E-mail the log immediately. |
| Apply | Apply the current settings. |
| Cancel | Clear the current settings. |

### Selecting What Information to Log

Besides the standard information that is listed in the previous two tables, you can choose to log additional information. Those optional selections are as follows:

- Attempted access to blocked sites
- Connections to the Web-based interface of the modem router
- Router operation (start up, get time, and so on).
- Known DoS attacks and port scans

### Saving Log Files on a Server

You can choose to write the logs to a computer running a syslog program. To activate this feature, select **Broadcast on LAN**, or enter the IP address of the server where the syslog file will be written.

## Examples of Log Messages

Following are examples of log messages. In all cases, the log entry shows the time stamp as day, year-month-date hour:minute:second.

### Activation and Administration

```
Tue, 2006-05-21 18:48:39 - NETGEAR activated
```

[This entry indicates a power-up or reboot with initial time entry.]

```
Tue, 2006-05-21 18:55:00 - Administrator login successful -
IP:192.168.0.2
Thu, 2006-05-21 18:56:58 - Administrator logout - IP:192.168.0.2
```

[This entry shows an administrator logging in and out from IP address 192.168.0.2.]

```
Tue, 2006-05-21 19:00:06 - Login screen timed out - IP:192.168.0.2
```

[This entry shows a time-out of the administrator login.]

```
Wed, 2006-05-22 22:00:19 - Log emailed
```

[This entry shows when the log was e-mailed.]

### Dropped Packets

```
Wed, 2006-05-22 07:15:15 - TCP packet dropped -
Source:64.12.47.28,4787,WAN - Destination:134.177.0.11,21,LAN - [Inbound
Default rule match]
Sun, 2006-05-22 12:50:33 - UDP packet dropped -
Source:64.12.47.28,10714,WAN - Destination:134.177.0.11,6970,LAN -
[Inbound Default rule match]
Sun, 2006-05-22 21:02:53 - ICMP packet dropped -
Source:64.12.47.28,0,WAN - Destination:134.177.0.11,0,LAN - [Inbound
Default rule match]
```

[These entries show an inbound FTP (port 21) packet, a User Datagram Protocol (UDP) packet (port 6970), and an Internet Control Message Protocol (ICMP) packet (port 0) being dropped as a result of the default inbound rule, which states that all inbound packets are denied.]

# Enabling Security Event E-mail Notification

To receive logs and alerts by e-mail, you must provide your e-mail information in the E-mail screen and specify which alerts you would like to receive and how often. In the main menu, under Security, select **E-mail**. The E-mail screen displays.

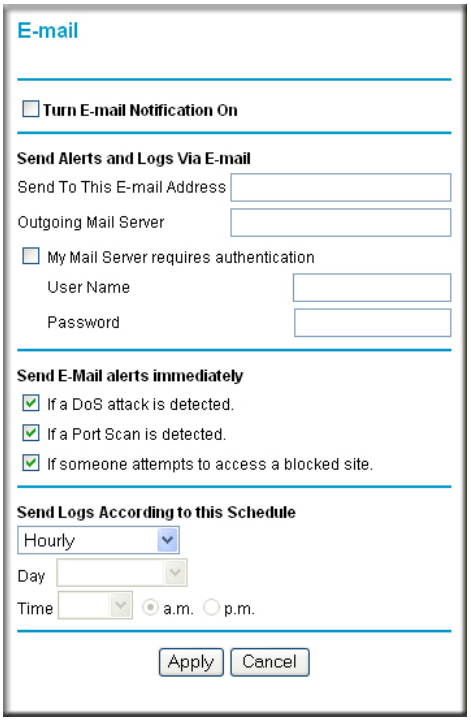



**Figure 4-9**

The E-mail screen allows you to make the following selections:

- **Turn E-mail Notification On**. Select this check box if you want to receive e-mail logs and alerts from the modem router.
- **Send To This E-mail Address**. Enter the e-mail address to which logs and alerts are sent. This e-mail address will also be used as the From address. If you leave this field blank, log and alert messages are not via e-mail.

- **Outgoing Mail Server**. Enter the name or IP address of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You might be able to find this information in the configuration settings of your e-mail program. Enter the e-mail address to which logs and alerts are sent. This e-mail address is also used as the From address. If you leave this field blank, log and alert messages are not sent by e-mail.
- **My Mail Server requires authentication**.If you use an outgoing mail server provided by your current ISP, you do not need to select this field. If you use an e-mail account that is not provided by your ISP, select this field, and enter the required user name and password information.
- **Send E-Mail alerts immediately**. Select the corresponding check box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.
- **Send Logs According to this Schedule**. Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
  - Day for sending log
    Specifies which day of the week to send the log. Relevant when the log is sent weekly.
  - Time for sending log
    Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

  If the Weekly, Daily or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, it is cleared from the modem router's memory. If the modem router cannot e-mail the log file, the log buffer might fill up. In this case, the modem router overwrites the log and discards its contents.

## Running Diagnostic Utilities and Rebooting the Modem Router

The modem router has a diagnostics feature. You can use the Diagnostics screen to perform the following functions from the modem router:

- Ping an IP address to test connectivity to see if you can reach a remote host.
- Perform a DNS lookup to test if an Internet name resolves to an IP address to verify that the DNS server configuration is working.
- Display the Routing table to identify what other modem routers the modem router is communicating with.

- Reboot the modem router to enable new network configurations to take effect or to clear problems with the modem router's network connection.

In the main menu, under Maintenance, select Diagnostics to display the following screen.

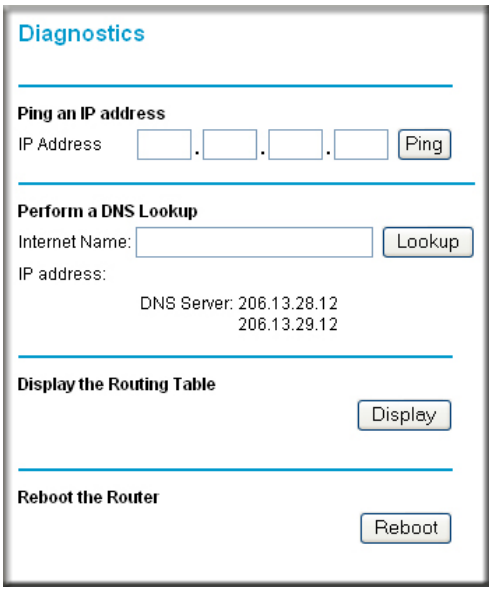



**Figure 4-10**

## Configuring Remote Management

Using the Remote Management screen, you can allow a user or users on the Internet to configure, upgrade, and check the status of your modem router.

**Note:** Be sure to change the modem router's default password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper case and lower case), numbers, and symbols. Your password can be up to 30 characters.

To configure remote management:

1. Log in to the modem router as described in "Logging In to the Modem Router" on page 1-2.
2. Under Advanced in the main menu, select Remote Management to display this screen:

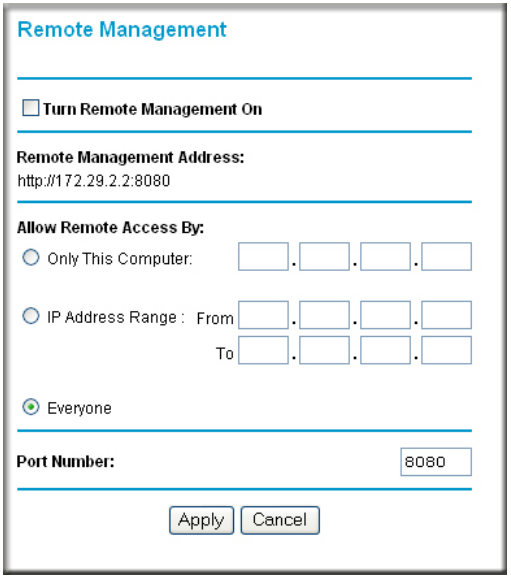



**Figure 4-11**

3. Select the **Turn Remote Management On** check box.
4. Specify what external addresses will be allowed to access the modem router's remote management. For security, restrict access to as few external IP addresses as practical:
   - To allow access from any IP address on the Internet, select **Everyone**.
   - To allow access from a range of IP addresses on the Internet, select **IP address Range**. Enter a beginning and ending IP address to define the allowed range.
   - To allow access from a single IP address on the Internet, select **Only this Computer**. Enter the IP address that will be allowed access.
5. Specify the port number that will be used for accessing the management interface.

   Web browser access usually uses the standard HTTP service port 80. For greater security, you can change the remote management Web interface to a custom port by entering that number in the field provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.
6. Click **Apply** to have your changes take effect.

   When accessing your modem router from the Internet, you will type your modem router's WAN IP address in your browser's **Address** field, followed by a colon (:) and the custom port

number. For example, if your external address is 134.177.0.123 and you use port number 8080, enter the following in your browser:

**http://134.177.0.123:8080**

| | |
|---|---|
| | **Note:** In this case, the http:// must be included in the address. |

## Automatic Firmware Recovery

Should the firmware become corrupted, the modem router automatically detects this situation and opens the following screen to enable you to recover the firmware.

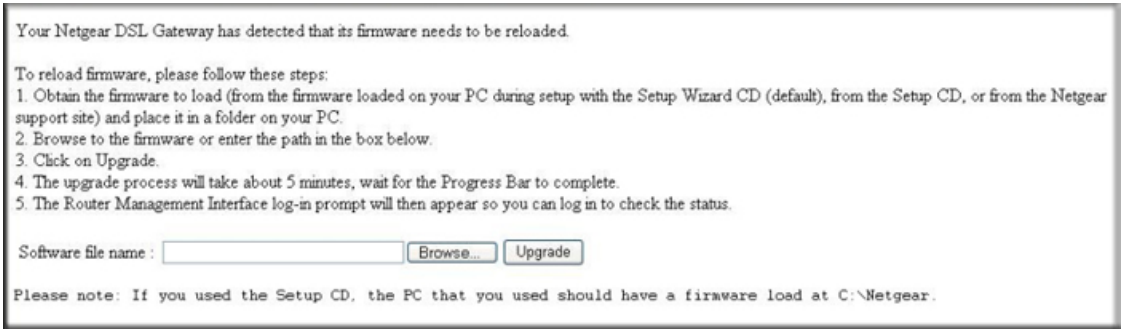

Your Netgear DSL Gateway has detected that its firmware needs to be reloaded.
To reload firmware, please follow these steps:
1. Obtain the firmware to load (from the firmware loaded on your PC during setup with the Setup Wizard CD (default), from the Setup CD, or from the Netgear support site) and place it in a folder on your PC.
2. Browse to the firmware or enter the path in the box below.
3. Click on Upgrade.
4. The upgrade process will take about 5 minutes, wait for the Progress Bar to complete.
5. The Router Management Interface log-in prompt will then appear so you can log in to check the status.
Software file name :
Browse...
Upgrade
Please note: If you used the Setup CD, the PC that you used should have a firmware load at C:\Netgear.

**Figure 4-12**

To recover the firmware:

1. If you already have the firmware file on your PC, go directly to step 2. If you do not have the firmware file on your PC, obtain the firmware from the NETGEAR support site at *http://www.netgear.com/support*.
2. Click **Browse**.
3. Navigate to the firmware file. (If you used the Setup CD, recovery firmware is located in the C:\Netgear directory.)
4. Click **Upgrade**.
5. The recovery process takes about 5 minutes. Wait for the progress bar to complete. After the firmware recovery is complete, the login screen for the Smart Wizard displays, allowing you to log in to the modem router to check its status.

# Chapter 5
# Advanced Configuration

This chapter describes how to configure the advanced features of your modem router. For information about remote management, see “Configuring Remote Management” on page 4-9. The following features are discussed in this chapter:


- “Configuring WAN Settings”
- “Setting up Quality of Service (QoS)” on page 5-3
- “Configuring LAN IP Settings” on page 5-7
- “Using Static Routes” on page 5-12
- “Configuring Universal Plug and Play” on page 5-15”
- “Building Wireless Bridging and Repeating Networks” on page 5-16
- “Displaying and Configuring Advanced WPS Settings” on page 5-22


## Configuring WAN Settings

### Setting Up a Default DMZ Server

The default demilitarized zone (DMZ) server feature is helpful when you use some online games and videoconferencing applications that are incompatible with NAT. The modem router is programmed to recognize some of these applications and to work correctly with them, but there are other applications that might not function well. In some cases, one local computer can run the application correctly if that computer’s IP address is entered as the default DMZ server.

**Note:** For security reasons, you should avoid using the default DMZ server feature. When a computer is designated as the default DMZ server, it loses much of the protection of the firewall, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

Incoming traffic from the Internet is usually discarded by the modem router unless the traffic is a response to one of your local computers or a service that you have configured in the Ports screen. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ server.

### How to Configure a Default DMZ Server

To assign a computer or server to be a default DMZ server:

1. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever user name, password, and LAN address you have chosen for the modem router.
2. In the main menu, under Advanced, select WAN Setup to display the following screen.

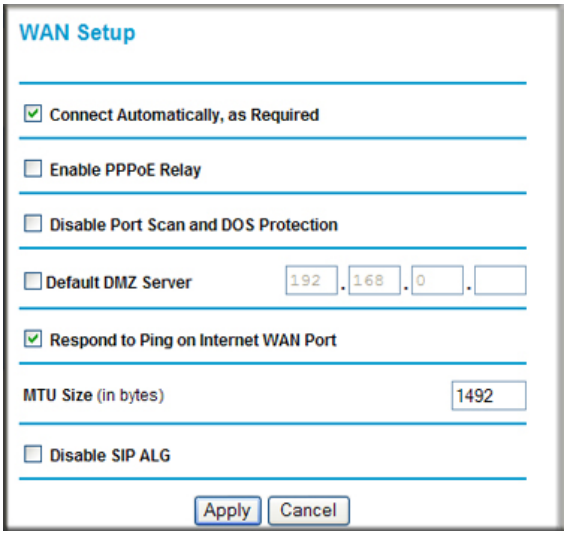



**Figure 5-1**

3. Select the **Default DMZ Server** check box.
4. Type the IP address for that server.
5. Click **Apply** to save your changes.

## Other WAN Options

The WAN Setup screen that is shown in Figure 5-1 also allows you perform the following tasks:

- **Connecting Automatically, as Required**

  Usually, this option should be enabled, so that an Internet connection is made automatically, whenever Internet-bound traffic is detected. If this causes high connection costs, you can disable this setting.

If this setting is disabled, you must connect manually, using the screen that you access by clicking the **Connection Status** button on the Status screen.

If you have an Always on connection, this setting has no effect.

- **Disabling Port Scan and DOS Protection**

  The firewall protects your LAN against port scans and denial of service (DOS) attacks. This protection should be disabled only in special circumstances.

- **Responding to a Ping on an Internet WAN Port**

  If you want the modem router to respond to a ping from the Internet, select the **Respond to Ping on Internet WAN Port** check box. This should be used only as a diagnostic tool, since it allows your modem router to be discovered. Do not select this check box unless you have a specific reason to do so.

- **Setting the MTU Size**

  The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs you might need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

- **Disabling the SIP ALG**

  The Session Initiation Protocol (SIP) Application Level Gateway (ALG) is enabled by default to optimize VoIP phone calls that use the SIP. The **Disable SIP ALG** check box allows you to disable the SIP ALG. Disabling the SIP ALG might be useful when running certain applications.

## Setting up Quality of Service (QoS)

Quality of Service (QoS) is an advanced feature that can be used to prioritize some types of traffic ahead of others. The modem router can provide QoS prioritization over the wireless link and on the Internet connection.

The modem router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application must be WMM enabled. Legacy applications that do not support

WMM, and applications that do not require QoS, are assigned to the best effort category, which receives a lower priority than voice and video.

# Configuring QoS for Internet Access

To specify prioritization of traffic, you must add or create a policy for the type of traffic. To go to the QoS Setup screen, from the main menu, under Advanced, select QoS Setup.

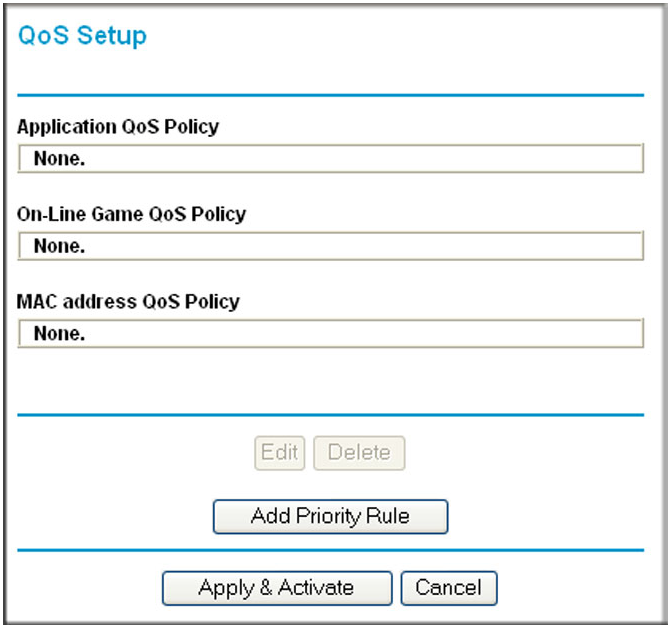



**Figure 5-2**

You can give prioritized Internet access to the following types of traffic:

- For specific applications or online games, see “QoS for Applications and Online Gaming” on page 5-4.
- For QoS from a specific device by MAC address, see “QoS for a MAC Address” on page 5-6.

## QoS for Applications and Online Gaming

To create a QoS policy for traffic for specific applications or online games:

**1.** From the main menu, under Advanced, select QoS Setup. The QoS Setup screen displays.

2. Click A**dd Priority Rule**. The QoS - Policy Rules screen displays:

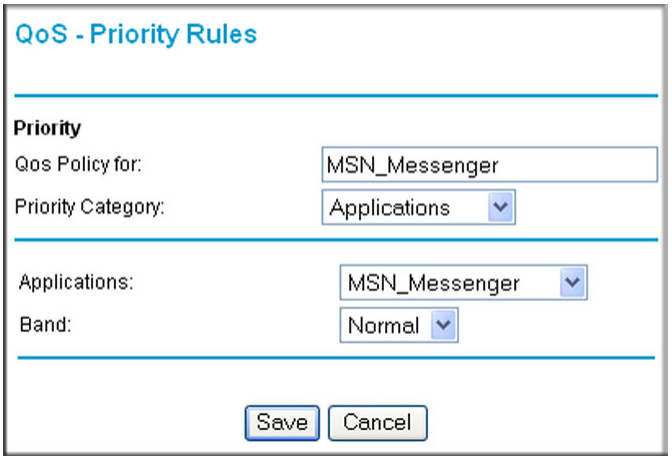



**Figure 5-3**

3. In the **Priority Category** field, either use the default selection of **Applications,** or select **Online Gaming** or **MAC Address**.

   A drop-down list of predefined applications or games is available.

4. You can select an existing item, or you can scroll to the bottom of the list and select **Add a New Application** or **Add a New Game**.

   **a.** If you chose to add a new entry, the screen expands as shown:

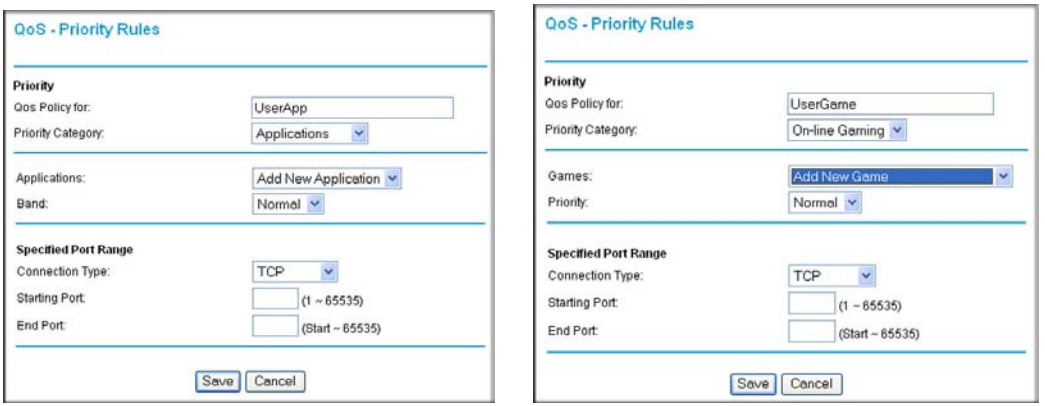



**Figure 5-4**

**b.** In the **QoS Policy for** field, enter a descriptive name for the new application or game.

**c.** Select the Connection Type, either **TCP, UDP,** or both (**TCP/UDP**), and specify the port number or range of port numbers used by the application or game.

**5.** Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.

**6.** In the QoS Setup screen, click **Apply & Activate**.

## QoS for a MAC Address

To create a QoS policy for traffic from a specific MAC address:

**1.** From the main menu, under Advanced, select QoS Setup. The QoS Setup screen displays.

**2.** Click **Add Priority Rule**.

**3.** In the **Priority Category** field, select **MAC Address**. The screen changes:

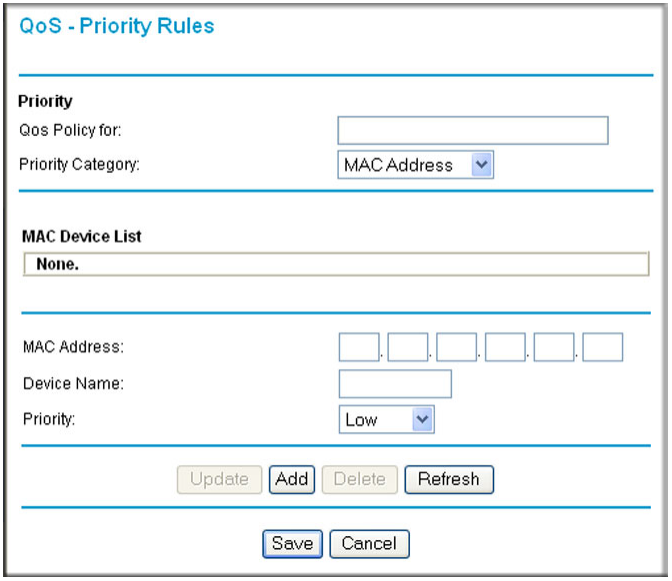



**Figure 5-5**

**4.** If the device to be prioritized appears in the **MAC Device List** field, select it. The information from the MAC Device List is used to populate the policy name, MAC Address, and Device Name fields. If the device does not appear in the MAC Device List, click **Refresh**. If it still does not appear, you must complete these fields manually.

5. From the **Priority** drop-down list, select the priority that this device's traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.
6. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
7. In the QoS Setup screen, click **Apply & Activate**.

## Editing or Deleting an Existing QoS Policy

To edit or delete an existing QoS policy:

1. From the main menu, under Advanced, select QoS Setup. The QoS Setup screen displays.
2. Select the radio button for the QoS policy to be edited or deleted, and do one of the following:
   - Click **Delete** to remove the QoS policy.
   - Click **Edit** to edit the QoS policy. Follow the instructions in the preceding sections to change the policy settings.
3. Click **Apply & Activate** in the QoS Setup screen so that your changes take effect.

# Configuring LAN IP Settings

The LAN IP Setup screen allows configuration of LAN IP services such as DHCP and RIP.

The modem router is shipped preconfigured to use private IP addresses on the LAN side, and to act as a DHCP server. The modem router's default LAN IP configuration is as follows:

- LAN IP address. 192.168.0.1
- Subnet mask. 255.255.255.0

These addresses are part of the Internet Engineering Task Force (IETF)–designated private address range for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes by opening the LAN IP Setup menu.

Under Advanced in the main menu, select LAN IP Setup.

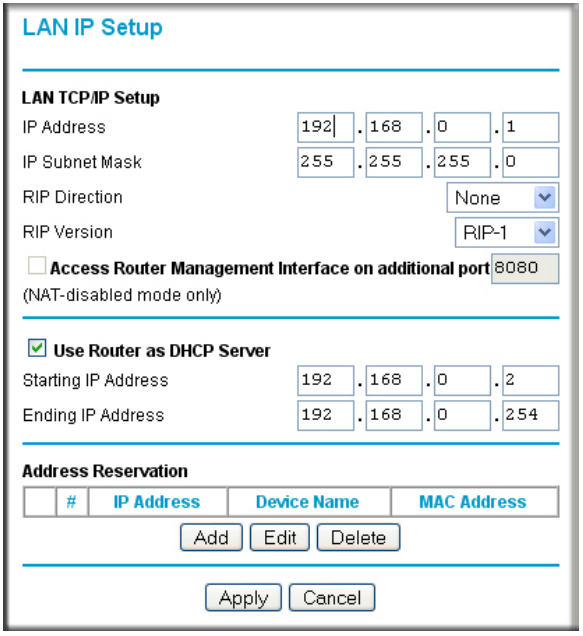



**Figure 5-6**

The LAN TCP/IP Setup settings are:

- **IP Address**. This is the LAN IP address of the modem router.
- **IP Subnet Mask**. This is the LAN subnet mask of the modem router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or modem router.
- **RIP Direction**. Router Information Protocol (RIP) allows a modem router to exchange routing information with other routers. The RIP Direction selection controls how the modem router sends and receives RIP packets. Both is the default setting.
  - When set to **Both** or **Out Only**, the modem router broadcasts its routing table periodically.
  - When set to **Both** or **In Only**, the modem router incorporates the RIP information that it receives.
  - When set to **None**, the modem router does not send any RIP packets and ignores any RIP packets received.

- **RIP Version**. This controls the format and the broadcasting method of the RIP packets that the modem router sends. It recognizes both formats when receiving. By default, this is set for RIP-1.
  - **RIP-1**. This version is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup.
  - **RIP-2**. This version carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format.
    - **RIP-2B**. This version uses subnet broadcasting.
    - **RIP-2M**. This version uses multicasting.
- **Access Router Management Interface on additional port**. When NAT is disabled, the modem router's management interface may be accessed at the modem router's LAN address using the port number you enter. This feature is not available when NAT is enabled.

**Note:** If you change the LAN IP address of the modem router while connected through the browser, you will be disconnected. You must then open a new connection to the new IP address and log in again.

## Configuring DHCP

By default, the modem router functions as a Dynamic Host Configuration Protocol (DHCP) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the modem router's LAN. The assigned default gateway address is the LAN address of the router. IP addresses are assigned to the attached PCs from a pool of addresses specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. See the online document that you can access from "TCP/IP Networking Basics" in Appendix B for an explanation of DHCP and information about how to assign IP addresses for your network.

### Use Router as DHCP Server

If another device on your network will be the DHCP server, or if you will manually configure the network settings of all of your computers, clear the **Use router as DHCP server** check box. Otherwise, leave it selected.

Specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.2 and 192.168.0.254, although you might want to save part of the range for devices with fixed addresses.

The router delivers the following settings to any LAN device that requests DHCP:

- An IP address from the range you have defined
- Subnet mask
- Gateway IP address is the router's LAN IP address
- Primary DNS server, if you entered a primary DNS address in the Basic Settings screen; otherwise, the router's LAN IP address
- Secondary DNS server, if you entered a secondary DNS address in the Basic Settings screen
- WINS server, short for *Windows Internet Naming Service Server*, determines the IP address associated with a particular Windows computer. A WINS server records and reports a list of names and IP address of Windows PCs on its local network. If you connect to a remote network that contains a WINS server, enter the server's IP address here. This allows your PCs to browse the network using the Network Neighborhood feature of Windows.

### How to Configure Reserved IP Addresses

When you specify a reserved IP address for a computer on the LAN, that computer will always receives the same IP address each time it access the router's DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

To reserve an IP address:

1. In the LAN IP Setup screen, click the **Add** button.
2. In the **IP Address** field, type the IP address to assign to the computer or server. Choose an IP address from the router's LAN subnet, such as 192.168.0.x.
3. Type the MAC address of the computer or server.

**Tip:** If the computer is already present on your network, you can copy its MAC address from the Attached Devices screen and paste it here.

4. Click **Apply** to enter the reserved address into the table.

**Note:** The reserved address will not be assigned until the next time the computer contacts the router's DHCP server. Reboot the computer or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry:

1. Click the button next to the reserved address that you want to edit or delete.
2. Click **Edit** or **Delete**.

## Configuring Dynamic DNS

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service that will allow you to register your domain to their IP address, and will forward traffic directed at your domain to your frequently changing IP address.

The router contains a client that can connect to a Dynamic DNS service provider. To use this feature, you must select a service provider and obtain an account with them. After you have configured your account information in the router, whenever your ISP-assigned IP address changes, your router automatically contacts your Dynamic DNS service provider, logs in to your account, and registers your new IP address.

To configure Dynamic DNS:

1. Log in to the modem router as described in "Logging In to the Modem Router" on page 1-2.
2. In the main menu, under Advanced, select Dynamic DNS to display the following screen.

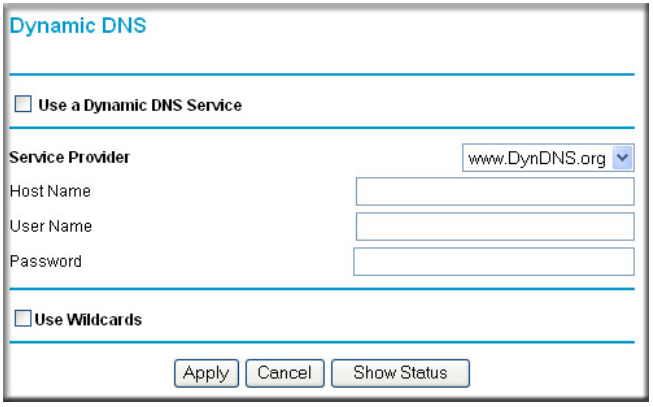



**Figure 5-7**

3. Access the website of one of the Dynamic DNS service providers whose names appear in the **Service Provider** drop-down list, and register for an account. For example, for dyndns.org, go to www.dyndns.org.

4. Select the **Use a dynamic DNS Service** check box.
5. Select the name of your Dynamic DNS service provider.
6. Type the host name that your Dynamic DNS service provider gave you. The Dynamic DNS service provider might call this the domain name. If your URL is myName.dyndns.org, then your host name is myName.
7. Type the user name for your Dynamic DNS account.
8. Type the password (or key) for your Dynamic DNS account.
9. If your Dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the **Use Wildcards** check box to activate this feature. For example, the wildcard feature causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.
10. Click **Apply** to save your configuration.

| | |
|---|---|
| | **Note:** If your ISP assigns a private WAN IP address such as 192.168.x.x or 10.x.x.x, the Dynamic DNS service will not work because private addresses will not be routed on the Internet. |

# Using Static Routes

Static routes provide additional routing information to your router. Under normal circumstances, the router has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You must configure static routes only for unusual cases such as multiple routers or multiple IP subnets located on your network.

## Static Route Example

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.0.100.
- Your company's network address is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the modem router, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on

the 134.177.0.0 network, your router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100. The static route setup would look like Figure 5-9.

In this example:

- The **Destination IP Address** and **IP Subnet Mask** fields specify that this static route applies to all 134.177.x.x addresses.
- The **Gateway IP Address** field specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.0.100.
- The value in the **Metric** field represents the number of routers between your network and the destination. This is a direct connection, so it can be set to the minimum value of 2.
- The **Private** check box is selected only as a precautionary security measure in case RIP is activated.

## Configuring Static Routes

1. Log in to the modem router as described in "Logging In to the Modem Router" on page 1-2.
2. In the main menu, under Advanced, select Static Routes to display the Static Routes table.

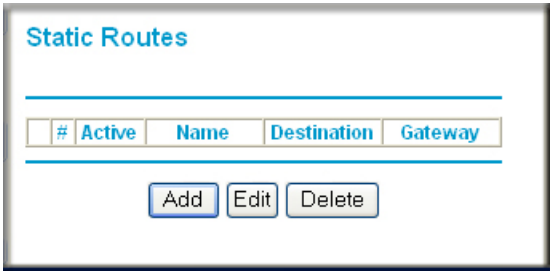



**Figure 5-8**

### To Add a Static Route

1. Click **Add** to open the following Static Routes screen.

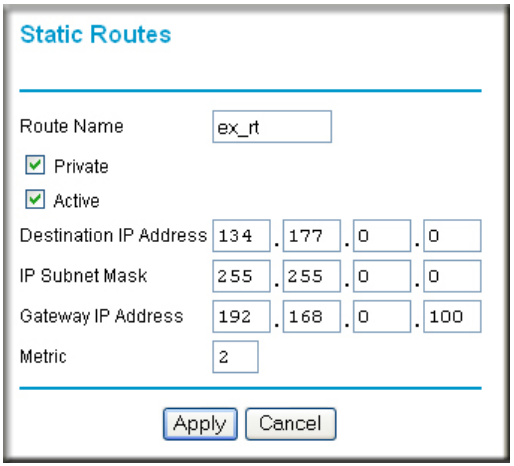



**Figure 5-9**

2. Enter a route name for this static route in the **Route Name** field. This name is for identification purpose only.
3. Select **Private** if you want to limit access to the LAN only. The static route will not be reported in RIP.
4. Select **Active** to make this route effective.
5. Enter the destination IP address of the final destination.
6. Enter the IP subnet mask for this destination. If the destination is a single host, type 255.255.255.255.
7. Enter the gateway IP address, which must be a router on the same LAN segment as the router.
8. Enter a number between 2 and 15 as the metric value in the **Metric** field. This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works.

**9.** Click **Apply**. The Static Routes table is updated to show the new entry.

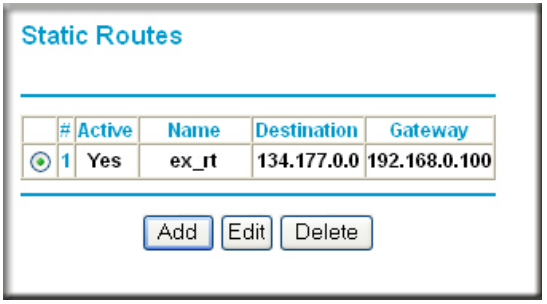



**Figure 5-10**

## Configuring Universal Plug and Play

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

**1.** Select UPnP on the main menu to display the UPnP screen:

**Figure 5-11**

2. Fill in the settings on the UPnP screen:

   - **Turn UPnP On**. UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If UPnp is disabled, the modem router does not allow any device to automatically control the resources, such as port forwarding (mapping), of the modem router.
   - **Advertisement Period**. The advertisement period is how often the modem router advertises (broadcasts) its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations might compromise the freshness of the device status but can significantly reduce network traffic.
   - **Advertisement Time To Live**. The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. A hop is the number of steps allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it might be necessary to increase this value a little.
   - **UPnP Portmap Table**. The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the modem router and which ports (internal and external) that device has opened. The UPnP Portmap Table also displays what type of port is opened and if that port is still active for each IP address.

3. To save, cancel your changes, or refresh the table:

   - Click **Apply** to save the new settings to the modem router.
   - Click **Cancel** to disregard any unsaved changes.
   - Click Refresh to update the portmap table and to show the active ports that are currently opened by UPnP devices.

## Building Wireless Bridging and Repeating Networks

With the DGN2000 modem router, you can build large bridged wireless networks that form an IEEE 802.11n Wireless Distribution System (WDS). Using the modem router with other access points (APs) and wireless devices, you can connect clients by using their MAC addresses rather than by specifying IP addresses.

Here are some examples of wireless bridged configurations:

- **Point-to-point bridge**. The modem router communicates with another bridge-mode wireless station. See "Point-to-Point Bridge Configuration."
- **Multi-point bridge**. The modem router is the "master" for a group of bridge-mode wireless stations. Then all traffic is sent to this master, rather than to other access points. See "Multi-Point Bridge."
- **Repeater with wireless client association**. Sends all traffic to the remote access point. See "Repeater with Wireless Client Association."

**Note:** The wireless bridging and repeating feature uses the default security profile to send and receive traffic.

To view or change these configurations, select Advanced Wireless Settings from the main menu:

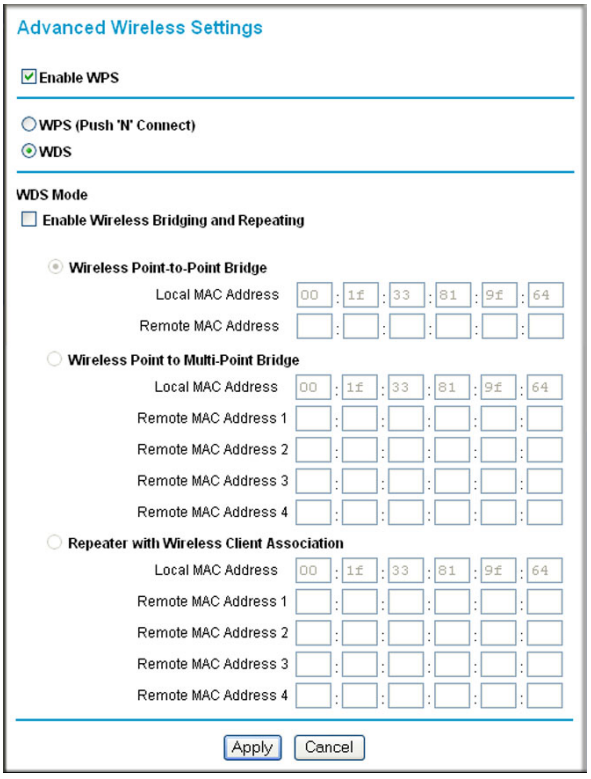



**Figure 5-12**

## Point-to-Point Bridge Configuration

In point-to-point bridge mode, the DGN2000 modem router communicates as an access point with another bridge-mode wireless station. As a bridge, wireless client associations are disabled—only wired clients can be connected. You must enter the MAC address of the other bridge-mode wireless station in the field provided. Use wireless security to protect this communication.

The following figure shows an example of point-to-point bridge mode.

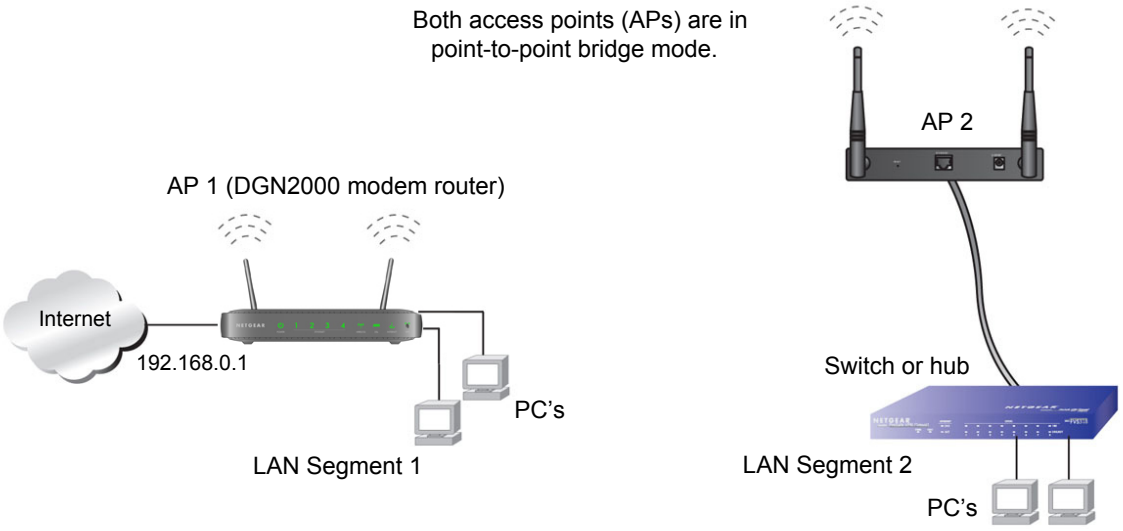



**Figure 5-13**

To set up a point-to-point bridge configuration (shown in Figure 5-13):

1. Configure the DGN2000 modem router (AP 1) on LAN Segment 1 in point-to-point bridge mode.
2. Configure the other access point (AP 2) on LAN Segment 2 in point-to-point bridge mode.

   The DGN2000 modem router must have AP 2's MAC address in its **Remote MAC Address** field, and AP 2 must have the DGN2000's MAC address in its **Remote MAC Address** field.
3. Configure both APs and verify that both APs are using he same SSID, channel, authentication mode, if any, and security settings if security is in use.
4. Disable the DHCP server on AP2. AP1 will then be the DHCP server.
5. Verify connectivity across LAN Segment 1 and LAN Segment 2. A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other PCs or servers connected to LAN Segment 1 or LAN Segment 2.

## Multi-Point Bridge

Multi-point bridge mode allows a modem router to bridge to multiple peer access points simultaneously. As a bridge, wireless client associations are disabled—only wired clients can be connected. Multi-point bridge mode configuration includes the following steps:

- Entering the MAC addresses of the other access points in the fields provided.
- Setting the other bridge-mode access points to Point-to-Point Bridge mode, using the MAC address of this DGN2000 as the Remote MAC Address.
- Using wireless security to protect this traffic.

The following figure shows an example of a multi-point bridge mode configuration.

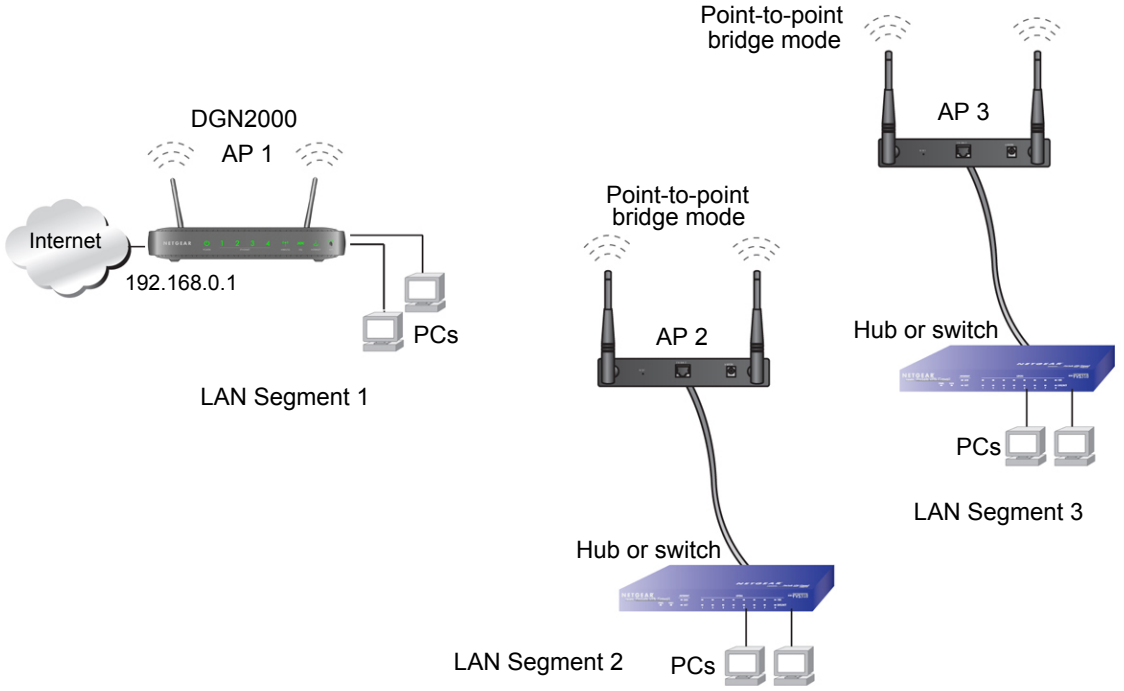



**Figure 5-14**

To set up the multi-point bridge configuration shown in Figure 5-14:

1. Configure the operating mode of the modem routers.
   - Because it is in a central location, configure the DGN2000 modem router (AP 1) on LAN Segment 1 in point-to-multi-point bridge mode, and enter the MAC addresses of AP-2 and AP-3 in the **Remote MAC Address 1** and **Remote MAC Address 2** fields.
   - Configure the access point (AP2) on LAN Segment 2 in point-to-point bridge mode with the remote MAC address of the DGN2000 modem router.
   - Configure the access point (AP3) on LAN Segment 3 in point-to-point bridge mode with the remote MAC address of the DGN2000 modem router.
2. Disable the DHCP server on AP2 and AP3. AP1 will then be the DHCP server.
3. Verify the following for all access points:
   - The LAN network configuration of the modem router and other access points are configured to operate in the same LAN network address range as the LAN devices.
   - Only one AP, the DGN2000 modem router in Figure 5-14, is configured in point-to-multi-point bridge mode; all the others are in point-to-point bridge mode.
   - All APs, including the DGN2000 modem router, must be on the same LAN. That is, all the AP LAN IP addresses must be in the same network.
   - If you are using DHCP, all access points should be set to **Obtain an IP address automatically (DHCP Client)** in the IP Address Source section of the Basic IP Settings screen.
   - All APs, including the DGN2000 modem router, must use the same SSID, channel, authentication mode, if any, and WEP security settings if security is in use.
   - All point-to-point APs must have the MAC address of AP 1 (the DGN2000 modem router in the previous figure) in the **Remote AP MAC address** field.
4. Verify connectivity across the LANs.
   - A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three LAN segments.

**Note:** Wireless stations configured as they are in Figure 5-14 will not be able to connect to the modem router or access points. If you require wireless stations to access any LAN segment, you can use additional access points configured in wireless access point mode in any LAN segment.

## Repeater with Wireless Client Association

In the repeater mode with wireless client association, the DGN2000 modem router sends all traffic to a remote AP. For the repeater mode, you must enter the MAC address of the remote “parent” access point. Alternatively, you can configure the DGN2000 modem router as the parent by entering the address of a “child” access point. Note that the following restrictions apply:

- You *do not* have the option of disabling client associations with this DGN2000 modem router.
- You cannot configure a sequence of parent/child APs. You are limited to only one parent AP, although if the DGN2000 modem router is the parent AP, it can connect with up to four child APs.

The following figure shows an example of a Repeater mode configuration.

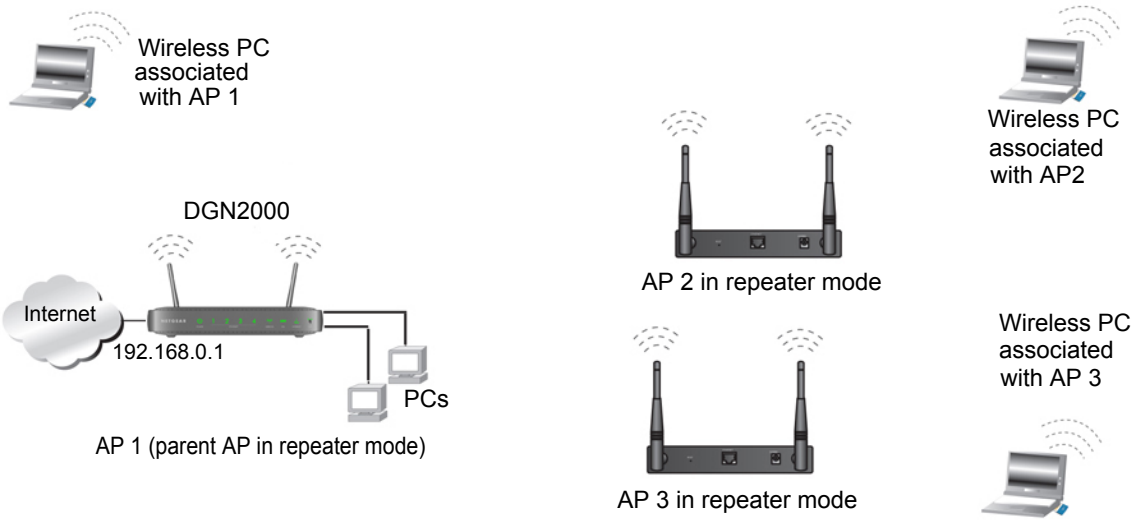



**Figure 5-15**

To set up a repeater with wireless client association:

1. Configure the operating mode of the devices.
   - Configure AP 1 (the DGN2000 modem router in Figure 5-15) on with the MAC address of AP 2 and AP 3 in the first two **Remote MAC Address** fields.
   - Configure AP 2 with the MAC address of AP 1 in the **Remote MAC Address** field.
   - Configure AP 3 with the MAC address of AP 1 in the **Remote MAC Address** field.

2. Verify the following for both access points:
   - The LAN network configuration of each AP is configured to operate in the same LAN network address range as the LAN devices.
   - The APs must be on the same LAN. That is, the LAN IP addresses for the APs must be in the same network.
   - If you are using DHCP, AP devices should be set to **Obtain an IP address automatically (DHCP Client)** in the IP Address Source section of the Basic IP Settings screen.
   - AP devices must use the same SSID, channel, authentication mode, and encryption.
3. Verify connectivity across the LANs. A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three WLAN segments.

## Displaying and Configuring Advanced WPS Settings

The advanced WPS settings cannot be displayed if you have selected WEP as the security option.. To display and specify advanced WPS settings:

1. Log in to the modem router as described in "Logging In to the Modem Router" on page 1-2.
2. In the main menu, under Advanced, select Advanced Wireless Settings to display the Advanced Wireless Settings screen. The following figure shows the upper part of the screen):

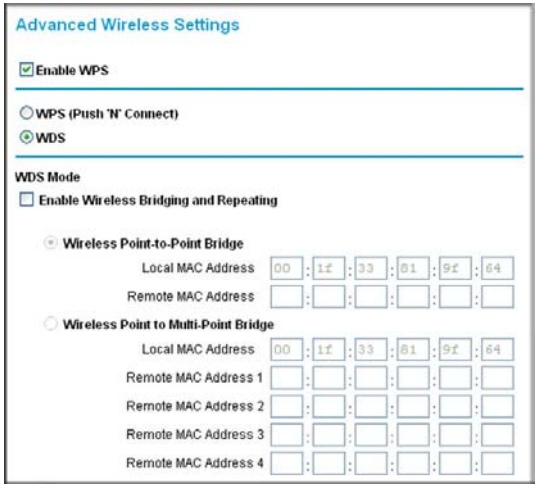

Advanced Wireless Settings
Enable WPS
WPS (Push 'N' Connect)
WDS
WDS Mode
Enable Wireless Bridging and Repeating
Wireless Point-to-Point Bridge
Local MAC Address
00 : 1f : 33 : 81 : 9f : 64
Remote MAC Address
Wireless Point to Multi-Point Bridge
Local MAC Address
00 : 1f : 33 : 81 : 9f : 64
Remote MAC Address 1
Remote MAC Address 2
Remote MAC Address 3
Remote MAC Address 4

**Figure 5-16**

By default the **Enable WPS check box** is selected. If you clear this check box and click **Apply** then you will not be able to use the Add a WPS Client feature or configure Advanced WPS settings.

3. Select the **WPS (Push 'N' Connect)** radio button to display the following screen:

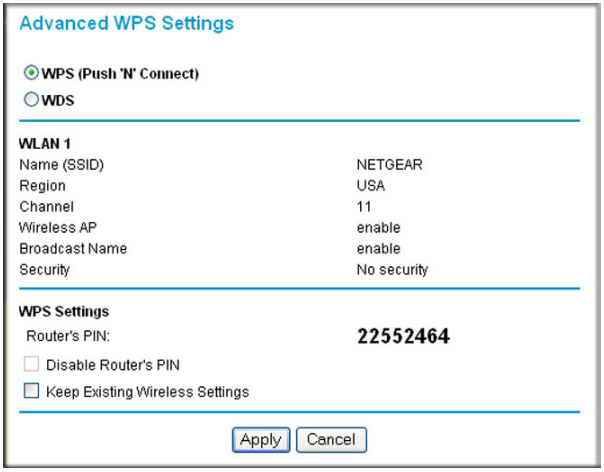



**Figure 5-17**

The WLAN1 settings are based on the selections that you made in the Wireless Settings screen. (See “Manually Configuring Your Wireless Network” on page 2-4). The following table explains the information displayed in the Advanced WPS Settings screen.

**Table 5-1. WLAN1 Settings and Router’s PIN**

| Field | Description |
|---|---|
| Name (SSID) | The service set ID, also known as the wireless network name for WLAN1. |
| Region | The country where the unit is set up for use. |
| Channel | The current channel, which determines the operating frequency. |
| Wireless AP | Indicates if the access point feature is enabled for WLAN1. If disabled, the Wireless LED on the front panel is off. |
| Broadcast Name | Indicates if the modem router is configured to broadcast its SSID for WLAN1. |
| Security | Indicates if security is configured on the modem router, and if so, what type of security is configured. |
| Router’s PIN | The PIN number that you use on a registrar (for example, from the Network Explorer on a Vista Windows PC) to configure the modem router’s wireless settings through WPS. You can also find the PIN on the modem router's product label. |

4. Under WPS Settings, you can configure the following settings:

   - **Disable Router's PIN**. Only when the modem router's PIN is enabled, you can configure the modem router's wireless settings or add a wireless client through WPS with the modem router's PIN number. The PIN function may temporarily be disabled when the modem router detects suspicious attempts to break into the modem router's wireless settings by using the modem router's PIN through WPS. You can manually enable the PIN function by deselecting the **Disable Router's PIN** check box.
   - **Keep Existing Wireless Settings**. By default, the **Keep Existing Wireless Settings** check box is cleared. This allows the modem router to automatically generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the modem router automatically selects this check box so that your SSID and wireless security settings remain the same if other WPS-enabled devices are added later.

     If you configure your wireless router settings and security manually, the **Keep Existing Wireless Settings** check box will also be enabled. This will allow you to use WPS (Push 'N' Connect) to connect additional WPS capable devices to your wireless network using the existing settings.

5. Click **Apply** to save your settings.

# Chapter 6
# Troubleshooting

This chapter provides information about troubleshooting your DGN2000 Wireless-N ADSL2+ Modem Router. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the router on?

  Go to "Basic Functioning."
- Have I connected the router correctly?

  Go to "Basic Functioning."
- I cannot access the router's configuration with my browser.

  Go to "Cannot Log in to the Modem Router" on page 6-3.
- I have configured the router but I cannot access the Internet.

  Go to "Troubleshooting the ISP Connection" on page 6-4.
- I cannot remember the router's configuration password.

  Go to "Restoring the Default Configuration and Password" on page 6-10.
- I want to clear the configuration and start over again.

  Go to "Restoring the Default Configuration and Password" on page 6-10.

## Basic Functioning

After you turn on power to the router, the following sequence of events should occur:

1. When power is first applied, verify that the Power LED is on.
2. After approximately 10 seconds, verify the following:
   a. The LAN port LEDs are lit for any local ports that are connected.
   b. The ADSL Link LED is lit.

If the ADSL link LED is lit, a link has been established to the connected device. If a LAN port is connected to a 100 Mbps device, verify that the port's LED is green. If the port is 10 Mbps, the LED is amber.

If any of these conditions does not occur, refer to the appropriate following section.

## "Welcome" Page Displays instead of Router Main Menu

This situation can occur if the CD Setup Wizard does not complete successfully; the unit will stay in "Wizard Mode". If the "Welcome" page displays instead of the main menu when you try to go to the Internet or log into the modem router, you can bypass the wizard using one of the following methods:

- Log into the modem router at **http://routerlogin.com/basicsetting.htm**.
- Perform a factory reset to take the router out of "Wizard Mode" altogether.

## Power LED Is Off

If the Power and other LEDs are off when your router is turned on:

- Make sure that the power cord is properly connected to your router and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12 V DC power adapter supplied by NETGEAR for this product.

If the error persists, you have a hardware problem and should contact Technical Support.

## Power LED Is Red

When the router is turned on, it performs a power-on self-test. If the Power LED turns red after a few seconds or at any other time during normal operation, there is a fault within the router. The Power LED also turns red when you press the Wireless On/Off and WPS buttons on the side panel of the modem router simultaneously for 6 seconds, and blinks red 3 times when you release these buttons. However, in this case, the modem router is working normally.

If the Power LED turns red to indicate a router fault, turn the power off and on to see if the modem router recovers.

If the power LED is still red 1 minute after power up:

- Turn the power off and on to see if the modem router recovers.
- Clear the router's configuration to factory defaults. This sets the router's IP address to 192.168.0.1. This procedure is explained in "Using the Wireless On/Off and WPS Buttons to Reset the Router" on page 6-10.

If the error persists, you might have a hardware problem and should contact Technical Support.

### LAN or ADSL Port LED Is Off

If either the LAN LEDs or ADSL Link LED does not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable: when connecting the ADSL port, use the cable that was supplied with the wireless-N modem router. If the ADSL link LED is still off, this may mean that there is no ADSL service or the cable connected to the ADSL port is bad.

### Window Appears Asking You to Reload Firmware

If a window appears with a message asking you to reload the firmware, this indicates that a problem has been detected with the current firmware. Please follow the on-screen instructions to access new firmware and reload the firmware into your router.

## Cannot Log in to the Modem Router

If you are unable to log in to the modem router from a computer on your local network, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in the previous section.
- Make sure that your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.0.2 to 192.168.0.254. Follow the instructions in the online document that you can access from "Preparing Your Network" in Appendix B for information about how to configure your computer.

- If your computer's IP address is shown as 169.254.x.x, recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router, and reboot your computer.
- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This sets the router's IP address to 192.168.0.1. This procedure is explained in "Using the Wireless On/Off and WPS Buttons to Reset the Router" on page 6-10.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.

If the router does not save changes you have made in the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another screen or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the Web browser. The changes might have occurred, but the Web browser might be caching the old configuration.

# Troubleshooting the ISP Connection

If your router is unable to access the Internet, you should check the ADSL connection, then the WAN TCP/IP connection.

## ADSL Link

If your router is unable to access the Internet, you should first determine whether you have an ADSL link with the service provider. The state of this connection is indicated with the Internet LED.

### ADSL Link LED Is Green or Blinking Green

If your ADSL link LED is green or blinking green, then you have a good ADSL connection. You can be confident that the service provider has connected your line correctly and that your wiring is correct.

### ADSL Link LED Is Blinking Amber

If your ADSL link LED is blinking amber, then your modem router is attempting to make an ADSL connection with the service provider. The LED should turn green within several minutes.

If the ADSL link LED does not turn green, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being sure to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green ADSL link LED, there might be a problem with your wiring. If the telephone company has tested the ADSL signal at your network interface device (NID), then you might have poor-quality wiring in your house.

### ADSL Link LED Is Off

If the ADSL link LED is off, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being sure to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green ADSL link LED, check for the following:

- Check that the telephone company has made the connection to your line and tested it.
- Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service. It might be necessary to use a swapper if your ADSL signal is on pins 1 and 4 or the RJ-11 jack. The modem router uses pins 2 and 3.

## Internet LED is Red

If the Internet LED is red, the device was unable to connect to the Internet. Verify the following:

- Check that your log-in credentials are correct, or that the information you entered on the Basic Settings screen is correct.
- Check with your ISP to verify that the Multiplexing method, VPI, and VCI settings on the ADSL settings screen are correct.
- Check if your ISP has a problem—it may not be the router that cannot connect to the Internet but your ISP that cannot provide an Internet connection.

## Obtaining an Internet IP Address

If your modem router is unable to access the Internet, and your Internet LED is green or blinking green, you should determine whether the modem router is able to obtain an Internet IP address from the ISP. Unless you have been assigned a static IP address, your modem router must request an IP address from the ISP. You can determine whether the request was successful using the browser interface.

To check the Internet IP address from the browser interface:

1. Launch your browser, and select an external site such as *www.netgear.com*.
2. Access the main menu of the modem router's configuration at http://192.168.0.1.
3. In the main menu, under Maintenance, click Router Status and check that an IP address is shown for the WAN port. If 0.0.0.0 is shown, your modem router has not obtained an IP address from your ISP.

If your router is unable to obtain an IP address from the ISP, the problem might be one of the following:

- If you have selected a login program, the service name, user name, or password might be incorrectly set. See the following section, "Troubleshooting PPPoE or PPPoA.
- Your ISP might check for your computer's host name.
  Assign the computer host name of your ISP account to the modem router in the browser-based Setup Wizard.
- Your ISP allows only one Ethernet MAC address to connect to Internet, and might check for your computer's MAC address. In this case, do one of the following:
  - Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.
  - Configure your router to spoof your computer's MAC address. This can be done in the Basic Settings screen. See the *Wireless-N ADSL2+ Modem Router DGN2000 Setup Manual*.

## Troubleshooting PPPoE or PPPoA

The PPPoE or PPPoA connection can be debugged as follows:

1. Access the main menu of the router at http://192.168.0.1.
2. Under Maintenance, select **Router Status**.
3. Click the **Connection Status** button.
4. If all of the steps indicate OK, then your PPPoE or PPPoA connection is up and working.

5. If any of the steps indicates Failed, you can attempt to reconnect by clicking **Connect**. The modem router will continue to attempt to connect indefinitely.

If you cannot connect after several minutes, you might be using an incorrect service name, user name, or password. There also might be a provisioning problem with your ISP.

**Note:** Unless you connect manually, the modem router will not authenticate using PPPoE or PPPoA until data is transmitted to the network.

## Troubleshooting Internet Browsing

If your modem router can obtain an IP address, but your computer is unable to load any Web pages from the Internet:

- Your computer might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the modem router's configuration, reboot your computer, and verify the DNS address as described in the online document that you can access from "Preparing Your Network" in Appendix B. Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer might not have the modem router configured as its TCP/IP modem router.

  If your computer obtains its information from the modem router by DHCP, reboot the computer, and verify the modem router address as described in the online document that you can access from "Preparing Your Network" in Appendix B.

## Resolving a 'Reload Firmware' Message

When you attempt to connect to the Internet, Windows may display a message that you must reload the router's firmware. If this situation occurs, a problem has been detected with the router's firmware.

To recover the firmware:

1. If you already have the firmware file on your PC, go directly to step 2. If you do not have the firmware file on your PC, obtain the firmware from the NETGEAR support site at *http://www.netgear.com/support*.
2. Click **Browse**.

3. Navigate to the firmware file. (If you used the Setup CD, recovery firmware is located in the C:\Netgear directory.)
4. Click **Upgrade**.
5. The recovery process takes about 5 minutes. Wait for the progress bar to complete. After the firmware recovery is complete, the login screen for the Smart Wizard displays, allowing you to log in to the modem router to check its status.

# Troubleshooting a TCP/IP Network Using the Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a TCP/IP network by using the ping utility in your computer.

## Testing the LAN Path to Your Modem Router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

To ping the router from a PC running Windows 95 or later:

1. From the Windows toolbar, click the **Start** button, and select **Run**.
2. In the field provided, type **Ping** followed by the IP address of the router, as in this example:

   **ping 192.168.0.1**
3. Click **OK**.

   You should see a message like this one:

   ```
   Pinging <IP address> with 32 bytes of data
   ```

   If the path is working, you see this message:

   ```
   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
   ```

   If the path is not working, you see this message:

   ```
   Request timed out
   ```

   If the path is not functioning correctly, you could have one of the following problems:

   - Wrong physical connections
     - Make sure that the LAN port LED is on. If the LED is off, follow the instructions in “LAN or ADSL Port LED Is Off” on page 6-3.

  - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.

- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

## Testing the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. In the Windows Run screen, type:

**PING -n 10 IP address**

where *IP address* is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your PC has the IP address of your router listed as the default modem router. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel. Verify that the IP address of the router is listed as the default modem router as described in the online document that you can access from "Preparing Your Network" in Appendix B.
- Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your PC, enter that host name as the account name in the Basic Settings screen.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your router to "clone" or "spoof" the MAC address from the authorized PC. Refer to your *Wireless-N ADSL2+ Modem Router DGN2000 Setup Manual*.

# Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router's administration password to **password** and the IP address to **192.168.0.1**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the Web Configuration Manager (see "Backing Up, Restoring, and Erasing Your Settings" on page 4-1).
- Press the Wireless On/Off and WPS buttons on the side panel of the router simultaneously for 6 seconds to reset the router to its factory default settings. Use this method for cases when the administration password or IP address is not known.

## Using the Wireless On/Off and WPS Buttons to Reset the Router

To restore the factory default configuration settings when you do not know the administration password or IP address, you must use the Wireless On/Off and WPS buttons on the side panel of the router:

1. Press and hold the Wireless On/Off and WPS buttons simultaneously until the Power LED turns red (about 6 seconds).
2. Release the Wireless On/Off and WPS buttons. The LED blinks red three times and then turn green when the router has reset to the factory default state. Wait for the router to reboot.

# Problems with Date and Time

In the main menu, under Security, select Schedule to display the current date and time of day. The modem router uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000.
  Cause. The router has not yet successfully reached a network time server. Check that your Internet access is configured correctly. If you have just completed configuring the router, wait at least 5 minutes, and check the date and time again.
- Time is off by one hour.
  Cause. The router does not automatically sense daylight savings time. In the Schedule screen, select the **Adjust for Daylight Savings Time** check box.

# Appendix A
# Technical Specifications

This appendix provides technical specifications for the DGN2000 Wireless-N ADSL2+ Modem Router.

## General Specifications

| Specification | | Description |
|---|---|---|
| **Network Protocol and Standards Compatibility** | | |
| | Data and routing protocols: | TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM |
| **Power Adapter** | | |
| | North America: | 120V, 60 Hz, input |
| | UK, Australia: | 240V, 50 Hz, input |
| | Europe: | 230V, 50 Hz, input |
| | All regions (output): | 12 V AC @ 1.0A output |
| **Physical** | | |
| | Dimensions: | 7.0" x 5.1" x 1.2"<br>177.5 mm x 130 mm x 31 mm |
| | Weight: | 0.58 lbs.<br>0.265 kg |
| **Environmental** | | |
| | Operating temperature: | 0° to 40° C (32º to 104º F) |
| | Operating humidity: | 10% to 90% relative humidity, noncondensing |
| | Storage temperature: | –20° to 70° C (–4º to 158º F) |
| | Storage humidity: | 5 to 95% relative humidity, noncondensing |
| **Regulatory Compliance** | | |
| | Meets requirements of: | FCC Part 15 Class B; VCCI Class B; EN 55 022 (CISPR 22), Class B |

| Specification | | Description |
|---|---|---|
| **Interface Specifications** | | |
| | LAN: | 10BASE-T or 100BASE-Tx, RJ-45 |
| | WAN: | ADSL, Dual RJ-11, pins 2 and 3<br>T1.413, G.DMT, G.Lite<br>ITU Annex A or B<br>ITU G.992.5 (ADSL2+) |

# Default Configuration

You can use the Wireless On/Off and WPS buttons located on the side panel of your router to reset all settings to their factory defaults. This is called a hard reset. To perform a hard reset, push and hold the Wireless On/Off and WPS buttons simultaneously for 6 seconds. Your router will return to the factory configuration settings shown in the following table.

| Feature | | Default Behavior |
|---|---|---|
| **Router Login** | | |
| | User login URL | *http://www.routerlongin.com* |
| | User name (case-sensitive) | admin |
| | Login password (case-sensitive) | password |
| **Internet Connection** | | |
| | WAN MAC address | Use default address |
| | WAN MTU size | 1500 |
| | Port speed | Autosensing |
| **Local Network (LAN)** | | |
| | Lan IP | 192.168.0.1 |
| | Subnet mask | 255.255.255.0 |
| | RIP direction | None |
| | RIP version | Disabled |
| | RIP authentication | None |
| | DHCP server | Enabled |
| | DHCP starting IP address | 192.168.0.2 |

| Feature | | Default Behavior |
|---|---|---|
| | DHCP ending IP address | 192.168.0.254 |
| | DMZ | Enabled or disabled |
| | Time zone | GMT |
| | Time zone adjusted for daylight savings time | Disabled |
| | SNMP | Disabled |
| **Firewall** | | |
| | Inbound (communications coming in from the Internet) | Disabled (except traffic on port 80, the http port) |
| | Outbound (communications going out to the Internet) | Enabled (all) |
| | Source MAC filtering | Disabled |
| **Wireless** | | |
| | Wireless communication | Enabled |
| | SSID name | NETGEAR |
| | Security | Disabled |
| | Broadcast SSID | Enabled |
| | Country/region | Europe |
| | RF channel | 6 |
| | Operating mode | Up to 130 Mbps |
| | Data rate | Best |
| | Output power | Full |
| | Access point | Enabled |
| | Authentication type | Open System |
| | Wireless card access list | All wireless stations allowed |

# Appendix B
# Related Documents

This appendix provides links to reference documents that you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

| Document | Link |
|---|---|
| TCP/IP Networking Basics | *http://documentation.netgear.com/reference/enu/tcpip/index.htm* |
| Wireless Networking Basics | *http://documentation.netgear.com/reference/enu/wireless/index.htm* |
| Preparing Your Network | *http://documentation.netgear.com/reference/enu/wsdhcp/index.htm* |
| Virtual Private Networking Basics | *http://documentation.netgear.com/reference/enu/vpn/index.htm* |
| Glossary: | *http://documentation.netgear.com/reference/enu/glossary/index.htm* |

# Index


## Numerics

128-bit WEP *2-14*

64-bit WEP *2-14*

## A

access lists *2-8, 2-10*

ADSL settings *1-9*

AES *2-9*

## B

backup configuration *4-1*

Basic Settings screen *1-7*

basic wireless connectivity *2-4*

## C

configuration
- backing up the configuration *4-1*
- erasing the configuration *4-2*
- manually configuring your ISP settings *1-6*

customer support *1-v*

## D

date and time *6-10*

daylight savings time *3-14, 6-10*

default DMZ server *5-1*

default reset buttons *6-10*

Denial of Service (DoS) protection *3-3*

DHCP *5-9*

diagnostics *4-14*

disabling SIP ALG *5-3*

DMZ server *5-1*

DNS server
- primary DNS server *1-5, 1-8*
- secondary DNS server *1-5, 1-8*

Dynamic DNS *5-11*

## E

ESSID *2-5*

## F

factory settings, restoring *4-2*

firewall rules
- inbound rules *3-6*
- order of precedence for firewall rules *3-11*
- outbound rules *3-9*

flash memory *4-3*

## H

host name *1-8*

## I

inbound firewall rules *3-6*

instant messaging *3-12*

Internet Service Provider (ISP) *1-2*

## L

LAN IP setup menu *5-8*

logging in to the modem router *1-2*

## M

MAC address
- configuring the MAC address *1-9*
- MAC address being rejected *6-9*

MAC address filter 2-12
MAC address spoofing 6-6
restricting wireless access by MAC address 2-13
manual configuration of your modem router 1-6
metric 5-14
multicasting 5-9
multi-point bridge mode 5-19

## N

Network Time Protocol 3-13, 6-10

## O

order of precedence for firewall rules 3-11
outbound firewall rules 3-9

## P

passphrase 2-15
password 1-5
ping 5-3
placement of your router 2-2
plug and play 5-15
point-to-point bridge mode 5-18
ports
port filtering 3-9
port forwarding 3-6
port numbers 3-12
PPPoE 1-5
primary DNS server 1-5, 1-8
primary wireless LAN 2-6
Push 'N' Connect (WPS) 2-16

## R

range of your wireless connection 2-2
remote management 4-15
repeater mode with wireless client association 5-21
reserved IP addresses 5-10
reset button 6-10
restore factory settings 4-2
restoring your password 6-10
restricting wireless access by MAC address 2-13
RIP 5-8
router status 4-4

## S

secondary DNS server 1-5, 1-8
sending logs by email 4-13
service blocking 3-9
service numbers 3-12
SIP ALG 5-3
Smart Wizard 1-1
SMTP 4-14
SSID 2-5, 2-8
syslog 4-12

## T

TCP/IP network troubleshooting 6-8
time of day 6-10
time zone 3-14
timeout, administrator login 3-3
time-stamping 3-14
TKIP 2-8
troubleshooting
general information 6-1
network troubleshooting 6-8
troubleshooting LEDs 6-3
trusted host 3-5

## U

upgrading firmware 4-3
usage statistics 4-4

## W

WEP authentication 2-13
Wi-Fi Protected Setup (WPS) 2-16
advanced settings 5-22
keep existing wireless settings 5-24

PIN method 2-18
push button method 2-17
router's PIN 5-24

WINS 5-10

wireless card access list 2-10

wireless encryption
WEP encryption 2-14
WPA encryption 2-15

wireless LAN 2-6

wireless mode
(up to) 130 Mbps 2-7
(up to) 270 Mbps 2-7
b only 2-7
g & b 2-7
g only 2-7

wireless security 2-3
disabled 2-8
mixed WPS-PSK+ WPA2-PSK 2-9
WEP 2-8
WPA2-PSK 2-9
WPA-802.1x 2-9
WPA-PSK 2-8

WLAN 4-7

World Wide Web 1-v